EUCLIDES

vakblad voor de wiskundeleraar

mei 09

nr 7

jaargang 84





Orgaan van de Nederlandse Vereniging van Wiskundeleraren

COLOFON

mei 09 nr 7

jaargang 84

Euclides is het orgaan van de Nederlandse Vereniging van Wiskundeleraren.

Het blad verschijnt 8 maal per verenigingsjaar.

ISSN 0165-0394



Inzendingen bijdragen

Artikelen en mededelingen naar de hoofdredacteur: Klaske Blom, Westerdoksdijk 39, 1013 AD Amsterdam

E-mail: redactie-euclides@nvvw.nl

Richtlijnen voor artikelen

Tekst liefst digitaal in Word aanleveren; op papier in drievoud. Illustraties, foto's en formules separaat op papier aanleveren: genummerd, scherp contrast.

Zie voor nadere aanwijzingen: www.nvvw.nl/euclricht.html

Realisatie

Ontwerp en vormgeving, fotografie, drukwerk en mailingservices

De Kleuver bedrijfscommunicatie b.v.

Veenendaal, www.dekleuver.nl

Nederlandse Vereniging van Wiskundeleraren

Website: www.nvvw.nl

Voorzitter

Marian Kollenveld,

Leeuwendaallaan 43, 2281 GK Rijswijk

Tel. (070) 390 70 04

E-mail: voorzitter@nvvw.nl

Secretaris

Kees Lagerwaard,

Eindhovensingel 15, 6844 CA Arnhem

Tel. (026) 381 36 46

E-mail: secretaris@nvvw.nl

Ledenadministratie

Elly van Bemmel-Hendriks,

De Schalm 19, 8251 LB Dronten

Tel. (0321) 31 25 43

E-mail: ledenadministratie@nvvw.nl

Helpdesk rechtspositie

NVvW - Rechtspositie-Adviesbureau,

Postbus 405, 4100 AK Culemborg

Tel. (0345) 531 324

Lidmaatschap

Het lidmaatschap van de NVvW is inclusief Euclides.

De contributie per verenigingsjaar bedraagt voor

- leden: € 57,50
- leden, maar dan zonder Euclides: € 35,00
- studentleden: € 28,00
- gepensioneerden: € 35,00
- leden van de VVWL: € 35,00

Bijdrage WwF (jaarlijks): € 2,50

Betaling per acceptgiro. Nieuwe leden dienen zich op te geven bij de ledenadministratie.

Opzeggingen moeten plaatsvinden vóór 1 juli.

Abonnementen niet-leden

Abonnementen gelden steeds vanaf het eerstvolgende nummer.

Niet-leden: € 55,00

Instituten en scholen: € 140,00

Losse nummers zijn op aanvraag leverbaar: € 17,50

Betaling per acceptgiro.

Advertenties en bijsluiters

De Kleuver bedrijfscommunicatie bv:

t.a.v. Annemieke Boere

Kerkewijk 63, 3901 EC Veenendaal

Tel. (0318) 555 075

E-mail: a.boere@dekleuver.nl

Kort vooraf

[Klaske Blom]

Memorabel

Om met een memorabel feit te openen: op 4 april hebben we Gert de Kleuver 'uitgegeten'. Na negen jaar heeft hij de redactievoorzittershamer neergelegd; hij vond het mooi geweest, het werd tijd voor iets nieuws. Uiteraard hebben we dit afscheid in zijn stijl gevierd, met een etentje. Gert was de man van de goede secundaire arbeidsomstandigheden: hij zorgde voor een plezierige vergadersfeer, voor een goed gesprek bij lunch of diner als dat nodig was, voor het snel verrekenen van de gemaakte reiskosten, kortom, voor omstandigheden waarin het inhoudelijke proces goed kon gedijen. Eén van zijn wapenfeiten – voor Euclides en het bestuur van de Vereniging letterlijk én figuurlijk van grote waarde – is het initiëren en implementeren van een goed advertentiebeleid. Zijn zakelijke instelling en instinct was een grote aanwinst. Gert, bedankt voor al het werk dat je voor Euclides hebt verzet!

Nieuwe programma's en gefundeerde didactiek

In mijn vorige stukje schreef ik dat staatssecretaris Van Bijsterveldt heeft ingestemd met de plannen van cTWO voor de nieuwe programma's in de Tweede Fase. Reden voor Paul Drijvers om u in een artikel te informeren over de voorgeschiedenis van de nieuwe programma's, over de belangrijkste overwegingen van de vernieuwingscommissie, de meest in het oog springende veranderingen en de plannen van cTWO voor de nabije toekomst. Veel interessante materie.
Zo ook in het vierde deel van de serie artikelen van Anne van Streun. Hij zoomt in op de didactiek van ons wiskundeonderwijs. Hij schrijft in de inleiding: 'We weten tegenwoordig veel over de manier waarop mensen informatie verwerken (…). Daar bestaat harde wetenschappelijke kennis over. Het wordt hoog tijd dat we die kennis benutten om de didactiek van ons vak steviger te funderen en de praktijk van elke dag in onze lessen, klassen en scholen vorm te geven op een meer wetenschappelijke basis.' Ik beveel dit artikel van harte bij u aan, net als dat van Lonneke Boels. In haar bijdrage noemt ze de staartdeling als symbool voor algoritmen die niet meer worden aangeleerd, en de problemen die daaruit voortvloeien. Na een analyse van verschillende manieren om een deling aan te pakken, komt ze tot een didactiek die het beste van twee werelden combineert. Wie kan het daar nu niet mee eens zijn?
Dat didactiek hoog op onze agenda staat, blijkt wel uit het grote aanbod van nascholingen en symposia. Om er enkele te noemen: het FI organiseert een nascholing kansrekening en statistiek waarbij o.a. de mogelijkheden in de klas centraal staan. Het APS organiseert een studiemiddag 'Van "ik snap het niet" tot dyscalculie' en gaat in op de vraag wat je als docent wel en vooral ook niet moet doen in je les. En half mei was het 'didactisch symposium' met presentaties door leraren die naast hun baan didactisch onderzoek doen. Ik weet het, deze opsomming is mosterd na de maaltijd en ik ben – misschien net als u – nergens geweest omdat ik 'gewoon' les moest geven. Maar de mogelijkheden om ons verder te bekwamen zijn er in overvloed. Houdt u de diverse websites en aankondigingen in de bladen in de gaten.

Tot slot

Zoals beloofd vindt u in dit nummer weer een stevig wiskundig artikel: Benne de Weger schrijft over cryptografie en het risico van het bestaan van zwakke sleutels. Boeiend en niet makkelijk, om stevig uw tanden in te zetten met potlood, gum en papier ernaast. Verder was ik weer 'op bezoek', dit keer bij het Ichthuscollege in Veenendaal, en sprak daar met twee collega's. De één met hart en ziel een vmbo-man, de ander te veel dictator(?) om een voorkeur te hebben.
Op de Verenigingspagina's treffen we dit keer bijdragen van drie bestuursleden! Ook Henk Bijleveld heeft de didactiek tot onderwerp van zijn schrijven gemaakt: hij signaleert een ontwikkeling in het wiskundeonderwijs op sommige vmbo-scholen die hem niet alleen maar vrolijk stemt. Kees Lagerwaard klapt weer uit de school van het bestuur en Henk van der Kooij roept u op om een bijdrage te leveren aan de studiedag in november.
En, last but not least, hoeveel insPIratie heeft u ontketend op 14 maart? Mooie foto's hè?!
Ik wens u veel sterkte met de laatste examenloodjes en weer veel leesgenoegen.
En mocht u ook een bijdrage willen leveren aan Euclides, dan weet u ons te vinden: *redactie-euclides@nvvw.nl* .

Inhoud

Aan dit nummer werkten verder mee:
Conny van den Brande en Hans Wisbrun.

Doorlopende Leerlijnen Rekenen en Wiskunde

DEEL 4: WAT WERKT WEL/NIET EN WAAROM DAN?

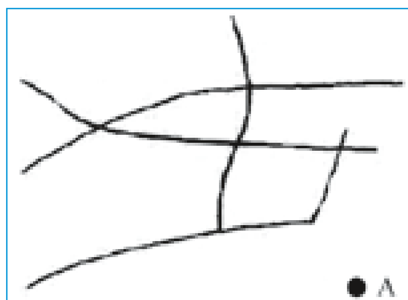
[Anne van Streun]

1. Oriëntatie

In de voorgaande delen van deze reeks[1] hebben we het gehad over het rapport *Doorlopende Leerlijnen Taal en Rekenen*[2], over de versterking van het programma voor de onderbouw havo/vwo[3] en over de brede problematiek van de aansluiting van algemeen vormend wiskundeonderwijs naar beroepsonderwijs of universitair onderwijs. In dit afsluitend artikel gaat het niet meer voornamelijk over de leerstof, maar over de didactiek waarmee wij in ons wiskundeonderwijs de gestelde doelen kunnen bereiken. We weten tegenwoordig veel over de manier waarop mensen informatie verwerken, informatie in het langetermijngeheugen vastleggen en vervolgens op het goede moment weer kunnen oproepen. Daar bestaat harde wetenschappelijke kennis over. Het wordt hoog tijd dat we die kennis benutten om de didactiek van ons vak steviger te funderen en de praktijk van elke dag in onze lessen, klassen en scholen vorm te geven op een meer wetenschappelijke basis. In onze onderlinge discussies kunnen en moeten we het stadium overstijgen van de persoonlijke opinies, vaak gebaseerd op de eigen leerervaringen als (hoog)leraar wiskunde. En die leerervaringen verschillen van die van onze modale leerlingen! Het is hoopgevend dat die harde wetenschappelijke kennis veelal goed spoort met de lespraktijken van erkend goede wiskundeleraren. Helaas worden die leraren vaak in de debatten over de kwaliteit en didactiek van ons wiskundeonderwijs overstemd door een vorm van retorisch geweld dat goed scoort in onze mediacultuur. Retorisch geweld dat zich niet houdt aan de regels van bewijsvoering, van redeneren in termen van oorzaken en gevolgen, aan het controleren van feiten en al die andere denkmethoden waar wij in de wiskunde zoveel waarde aan hechten.

2. Kennis opgeslagen in schema's

Ter illustratie gebruiken we plaatjes van Richard Skemp[4], die hij dertig jaar geleden gebruikte bij zijn lezing op de jaarlijkse studiedag van de Nederlandse Vereniging van Wiskundeleraren. Skemp was een psycholoog, wiskundige en didacticus op wiens werk in Nederland door Joop van Dormolen en andere wiskundedidactici is voortgebouwd[5]. Veel van wat hij indertijd al betoogde en opschreef, is in deze dertig jaar bevestigd door psychologisch onderzoek naar het leren van mensen en de werking van het geheugen. Een standaardwerk als *How people learn*[6] ondersteunt zonder meer zijn betoog van dertig jaar geleden, evenals de overzichtspublicatie *Adding it Up*[7], toegespitst op wiskunde leren en onderwijzen.
We gaan naar ***figuur 1***.



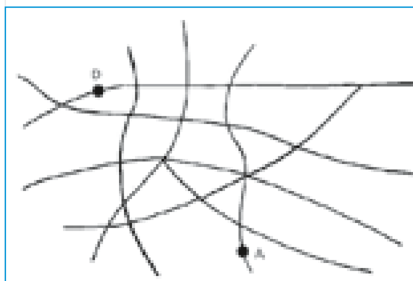
figuur 1 Wat is relevante kennis?

A stelt een situatie, opgave of probleem voor. Je neemt het waar, je leest het en je ziet het, je moet er iets mee, je vraagt je af of je er iets over weet. Je *werkgeheugen*, dat is je actueel beschikbare geheugenruimte waarmee je denkt, neemt *A* op. Dat werkgeheugen probeert een verbinding te leggen met wat je al weet, je *langetermijngeheugen*, een netwerk van feiten, begrippen, regels, verbindingen, routines. Het werkgeheugen wordt gebruikt om onmiddellijk informatie van de buitenwereld (hier door *A* aangeduid) te *bewerken* en te *verwerken*, terwijl het werkgeheugen input uit het langetermijngeheugen kan ontvangen. De relatie tussen het probleem *A* en het hopelijk bestaande kennisschema in je langetermijngeheugen is nog niet gelegd. Als die koppeling niet onmiddellijk associatief tot stand komt, dan kan de zoektocht naar relevante kennis worden ondersteund door het verkennen van de situatie *A*, het toepassen van heuristieken, zoals plaatjes schetsen en een getallenvoorbeeld proberen. Tijdens die *probleemverkenning* kan de gegeven situatie *A* worden gekoppeld aan een relevant schema uit het langetermijngeheugen, zoals gevisualiseerd ***in figuur 2***.

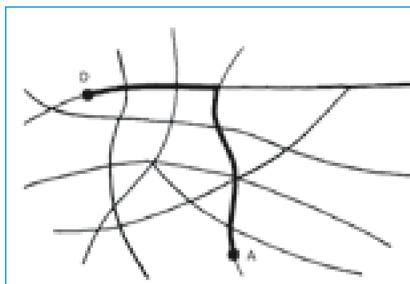


figuur 2 Koppeling aan bestaande kennis

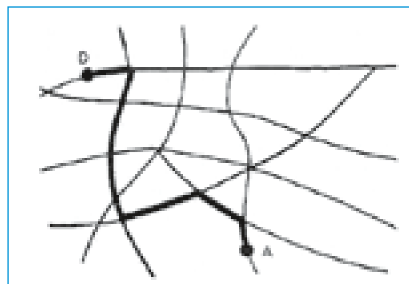
Je identificeert probleem *A*, je herinnert je iets, je denkt te weten waar het mee te maken heeft, een eerste bijpassend schema wordt opgeroepen uit je langetermijngeheugen. Dit is nog globaal, je plaatst situatie *A* in een bepaald gebied van je geheugen waar je iets over weet. Hier gaat al vaak iets mis, als je geen aandacht hebt voor enige verkenning van het probleem, van de situatie. Voor veel leerlingen en/of studenten betekent deze fase soms het oproepen van een heel arm schema; iets van, oh ja, ik moet wegstrepen. Of, er was iets met op nul herleiden. Daarover later meer.



figuur 3 De weg van A naar D vinden



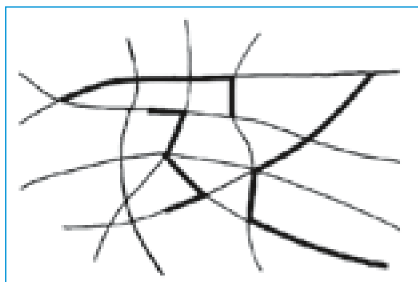
figuur 4a



figuur 4b

Vaak moet je iets doen met de gegeven situatie, een probleem oplossen, een antwoord vinden een doel bereiken. ***Zie figuur 3***. Ik ben in *A* en ik moet naar *D*. Hoe kom ik daar? Heb ik iets in huis, in mijn langetermijngeheugen, waarmee ik die weg kan vinden?
Soms moet ik een plan maken, bedenken wat ik achtereenvolgens moet doen. Hier zijn we al in het gebied van de *probleemaanpak*. Wat helpt mij om die weg te vinden? Het kan zo (***zie figuur 4a***), maar het kan ook anders (***zie figuur 4b***).

Zo zijn er meerdere routes in een bepaald kennisgebied die *vaak* kunnen worden bewandeld. Dat zijn de *routines*, snel op te roepen, feilloos uit te voeren, gememoriseerd, een belangrijk facet van ‘weten dat’; paraat hebben en paraat houden. Kun je een probleem of situatie na verkenning direct koppelen aan een *relevante routine* om een deelhandeling bijna automatisch uit te voeren, dan houd je ruimte over in je werkgeheugen om aan het eigenlijke probleem te werken (***zie figuur 5***). Kun je dat niet en moet je ook die deelhandeling opnieuw heruitvinden, dan verlies je intussen het zicht op het eigenlijke probleem. Want je werkgeheugen raakt overbelast.



figuur 5 Relevante routines

3. Losgeraakte of betekenisrijke routines

We komen nu bij een serieus didactisch probleem, dat Freudenthal in 1980 op het internationaal congres over wiskunde-onderwijs (ICME, 1980) tot één van de hoofdproblemen van de wiskundedidactiek benoemde. Afzonderlijk trainen en oefenen, zonder samenhang met andere begrippen en methoden kan leiden tot onbegrip!
En niet oefenen leidt tot een te zwakke beheersing. Links het voorbeeld rechts 25 analoge opgaven. Dat werkt voor het inoefenen van de procedure, maar het is niet wendbaar voor de situaties waarin je die procedure nodig hebt. In plaats van een kennisschema waarin de routines in samenhang en gekoppeld aan betekenissen in het langetermijngeheugen zijn opgeslagen, zijn de routines losgeraakt van hun betekenis en worden ze afzonderlijk opgeslagen; ***zie figuur 6***.



figuur 6 Losgeraakte routines

De bijbehorende instructiestrategie is: *VNO – Voordoen, Nadoen, Oefenen*. Opsplitsen van de leerstof in kleine eenheden, voordoen van eenvoudige voorbeelden, na laten doen onder controle, oefenen van een reeks analoge sommen opklimmend in moeilijkheid. Leerlingen kunnen snel zelf aan de slag, snel succes is mogelijk, het werkt goed op korte termijn en het is eenvoudig te toetsen. En er is weinig professionele kennis nodig van de leraar. Leerlingen kunnen alleen dat bepaalde type opgaven maken, het gaat alleen om reproductie, de kennis wordt gefragmentariseerd zonder samenhang en elk nieuw type opgave vereist een nieuw leerproces. Naarmate de leerlingen meer en meer routines moeten verwerven, blijken die losgeraakte routines steeds slechter uit het langetermijngeheugen te kunnen worden opgeroepen. Het aantal associatieve Pavlov-reacties neemt toe, omdat de routines ook losgeraakt raken van het type opgave waar ze voor zijn bedoeld.
Zo blijken voor veel leerlingen de formele rekenregels, bijvoorbeeld bij breuken, lastig te koppelen aan de situaties waar ze voor gelden. Hetzelfde geldt voor allerlei routines voor het oplossen van vergelijkingen en ongelijkheden. Het kennisschema in hun langetermijngeheugen lijkt wel een enorme chaos aan situaties en technieken die amper zinvol met elkaar kunnen worden verbonden. Het overzicht ontbreekt, de structuur is onzichtbaar, kernbegrippen zijn ondergesneeuwd door ad-hoc-technieken.
Wat doen we daar aan in ons onderwijs? Zoals Wim Bos[8] terugkijkend op zijn werk in 1984 betoogde, geldt ook voor de algebra dat de verworven kennis van de leerlingen moet worden aangevuld door systematisch te werken aan een versterking van de samenhang, het *overzicht* op allerlei methoden en situaties. Van globaal naar meer specifiek, zoekrichtingen opsporen (***zie figuur 7***).



figuur 7 Zoekrichtingen in de chaos

Een citaat:
‘Naar mijn mening moet de leerling op den duur in zijn langetermijngeheugen kunnen beschikken over een flink aantal zoekrichtingen en moet een bepaalde probleemsituatie *die* methoden activeren die bruikbaar zijn. Om dit te bereiken is het wenselijk dat de leerlingen eerst *ervaren* hebben dat je hersens gebruiken vaak

effectiever is dan zoeken in het geheugen naar formules of algoritmen. Deze ervaring kunnen ze het beste opdoen met wat ik noem *systematische heuristieken*, overzichten van mogelijkheden.'

Vervolgens geeft Bos dan als voorbeeld een overzicht voor het oplossen van goniometrische vergelijkingen:

Ga na of je de vergelijking kunt herleiden tot één van de volgende vier vormen:

1. Tot sin… = sin…, cos… = cos… of tan… = tan…
   Bijvoorbeeld: $\sin x = \cos(x - \frac{1}{4}\pi)$.
2. Op nul herleiden en ontbinden.
   Bijvoorbeeld: $\sin 2x = 2\cos x$.
3. Herleiden tot een vorm waarin maar één goniometrische verhouding voorkomt.
   Bijvoorbeeld: $\cos 2x = 2\sin x - 3\sin^2 x$.
4. Herleiden tot de vorm
   $a\cos x + b\sin x = c$.

Als het goed is, schrijft Bos, gaat het hier om een *ordening* van door ervaring verworven kennis van methoden; een ordening die in het geheugen aanwezig moet zijn, niet letterlijk uit het hoofd geleerd, maar schematisch als vier zoekrichtingen waaraan gedacht kan worden.

In het katern *Vergelijkingen vergelijken* van het *Handboek Didactiek van de Wiskunde* [9] komt dezelfde strategie voor in een poging om het grote gebied van allerlei typen vergelijkingen in de bovenbouw havo/vwo te herordenen in een operationele vorm. Op dezelfde manier helpen goede leraren leerlingen met het ordenen van allerlei typen verbanden en functies met de kenmerken van hun grafieken. Zoals al in de vorige artikelen is betoogd, is het essentieel dat leerlingen die verschillende typen vergelijkingen, functies enzovoort met hun kenmerken paraat moeten hebben.

4. De relatie tussen wiskunde en de werkelijkheid

Waarom moet wiskunde een basisvak in elk algemeen vormend curriculum zijn? Over welke inhouden hebben we het eigenlijk?

In de geschiedenis van het onderwijs in rekenen en wiskunde zijn daarop verschillende antwoorden gegeven. In Nederland hebben we al lang geleden ervoor gekozen om een zwaar accent te leggen bij het functioneren van de wiskundige kennis en vaardigheden buiten het vakgebied.

De schoonheid van het getalsysteem, de historische waarde van de meetkunde, de culturele waarde, het leren redeneren of denken, het bleek voor rekenen en wiskunde in Nederland niet genoeg voor de bepaling van de inhouden.

Het rekenen stond heel lang in functie van het cijferen, lange rijen berekeningen heel overzichtelijk en foutloos uitvoeren, want maatschappelijk was dat heel belangrijk.

Tegenwoordig ligt de nadruk veel meer bij het *functioneel gebruiken* van die kennis en routines in allerlei situaties. Die terechte keuze voor het leggen van een stevige verbinding met de buitenwereld lijkt evenwel te leiden tot een voor leerlingen redelijk chaotisch beeld van wat er in wiskunde aan de orde is. De strakke structuur van de meeste wiskundige deelgebieden heeft de charme van de eenvoud en het overzicht, maar bleek in het verleden in de hoofden van de meeste leerlingen tot een afgesloten systeem te leiden, waardoor de transfer naar toegepaste situaties slecht verliep. Te verwachten, want in het leerproces waren die situaties niet inbegrepen en behoorden ze niet tot het schema in het langetermijngeheugen.

Op dit moment zien we een totaal door elkaar lopen van allerlei soorten opgaven, situaties, formele rekenregels, intuïtieve methoden enzovoort. We zitten in de onderwijspraktijk van het rekenonderwijs en het wiskundeonderwijs met schoolboeken en ander lesmateriaal waarin het zelfs voor leraren lastig is om de kernen en doorlopende leerlijnen op te sporen. Laat staan voor de leerlingen. Dat vraagt om een bezinning op de vraag hoe we de transfer kunnen bevorderen vanuit de wiskunde naar alle gebieden waar we het gebruik van die wiskunde willen optimaliseren.

Met het oog op die vraag is het relevant om te kijken naar de zogenoemde *context-concept* benadering in de discussie over de vernieuwing van het onderwijs in de wiskunde en natuurwetenschappen. Een moeilijkheid in een brede discussie over de relatie tussen concepten en contexten is dat de termen *concept* en *context* in biologie, natuurkunde, scheikunde en wiskunde verschillend worden gebruikt, zodat het lastig is om een gemeenschappelijke lijn te vinden.

Beperken we ons tot het onderwijs in rekenen en wiskunde, dan is er een duidelijk negatieve reactie te constateren op de vertaling van Freudenthals ideeën

over *horizontaal mathematiseren* (wiskunde in relatie met de buitenwereld) en *verticaal mathematiseren* (verdiepen en abstraheren binnen de wiskunde) in het lesmateriaal voor rekenen en wiskunde. Beperken we ons tot de rol van contexten in dat lesmateriaal, dan is er veel kritiek op 'flauwe en onrealistische' verhaaltjessommen.
Een deel van de critici trekt de uiterste consequentie en kiest voor de weg terug, gewoon weer kaal en ouderwets rekenen met getallen en variabelen. Wellicht is het verhelderend om onderscheid te maken tussen de verschillende didactische functies van contexten. Het gaat om:

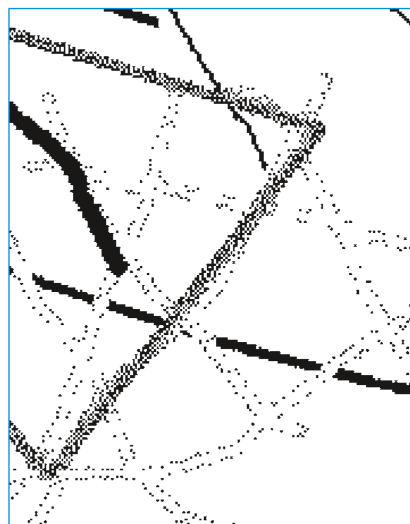
- *Contexten als denkmodel*;
- *Contexten om transfer te bevorderen*;
- *Contexten om (toegepaste) problemen op te lossen*;
- *Contexten om te leren modelleren*.

5. Contexten als denkmodel

Het gaat hier om *betekenisrijke contexten,* dat zijn situaties, problemen, vraagstellingen, uitspraken die voor leerlingen *betekenis krijgen* terwijl ze er mee aan het werk gaan. Goede contexten met deze functie worden gekenmerkt door een groot potentieel aan relaties met ervaringen van leerlingen *binnen* of *buiten* het wiskundeonderwijs. Ze omvatten *zowel* wiskundige als toegepaste probleemstellingen. Deze contexten, te kiezen uit de leefwereld, uit andere disciplines of uit de wiskunde, zijn bedoeld om het begrijpen van een concept of methode voor te bereiden en krijgen door de opgeroepen activiteiten betekenis voor leerlingen. De hier bedoelde contexten kunnen mits goed gekozen functioneren als *denkmodel of ankerpunt voor het geheugen*, aan de hand waarvan een cognitief schema wordt opgebouwd waarin *onderliggende concepten* centraal staan.

Contexten als denkmodellen voor functies

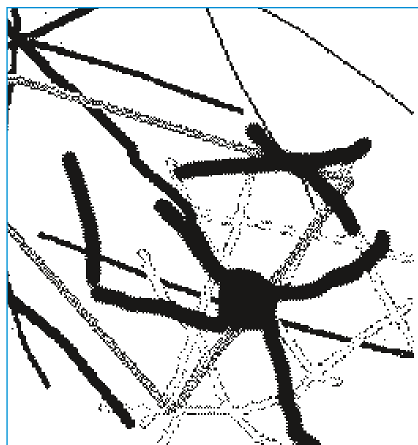
In de eerste leerjaren van het voortgezet onderwijs is een context met vaste en variabele kosten, gekoppeld aan een symbolische representatie met rekenpijlen, een goed denkmodel voor lineaire verbanden.
Na een brede verkenning van allerlei situaties, gekoppeld aan kenmerken van tabellen, grafieken en formules (horizontaal mathematiseren) volgt een explicitering in termen van formules en vergelijkingen. Een specifieke eerstegraads functie is tenslotte lid van een familie van eerstegraads functies en element van een brede verzameling functies (verticaal mathematiseren).
Bij tweedegraads functies gaat het veel meer om een directe studie van de verschillende vormen van de formules en de bijbehorende kenmerken van de grafieken (verticaal mathematiseren) zonder contexten van buiten de wiskunde als denkmodel. Plaatjes van spuitende fonteinen en voorbeelden van kwadratische groei (bijvoorbeeld van een oppervlakte) zijn niet kenmerkend genoeg om als denkmodel voor een nieuw schema te gaan functioneren.



figuur 8 Contexten

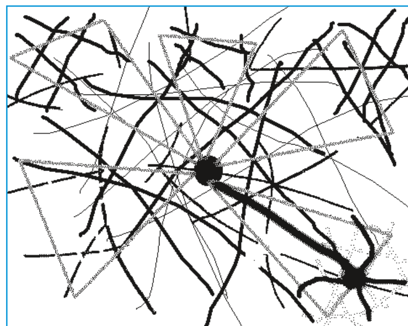
Een goed voorbeeld van de opbouw van een schema dat wel rijk is aan betekenissen, is dat van exponentiële groei. We beginnen met procentuele groei in relevante contexten te bestuderen en daar aan te rekenen (***zie figuur 8***).
Vervolgens gaan we het onderliggende concept opsporen. Kennelijk gaat het altijd om een *vermenigvuldigingsfactor* (bij 25% toename hoort de factor 1,25) en de *startwaarde*. Het *kernconcept* van exponentiële groei wordt in woorden samengevat: de groeifactor per tijdseenheid is steeds dezelfde. Allerlei andere contexten (zoals de groei van bacteriekolonies) komen in beeld.
In tabellen die het verband tussen twee grootheden beschrijven, wordt onderzocht of er sprake is van exponentiële groei. De exponentiële formule met beginhoeveelheid en groeifactor wordt opgesteld en geïnterpreteerd. Centraal staat het kernconcept dat steeds weer onder woorden moet worden

gebracht. Vanuit dat kernconcept worden steeds weer andere situaties onderzocht. De dominantie van dat kernconcept (***zie figuur 9***), waar de leraar, de opgaven en de toetsen steeds op terugkomen, bepaalt de sterkte van de structuur van het opgebouwde schema in het langetermijngeheugen. En zoals altijd hebben sommige leerlingen genoeg aan een enkel voorbeeld en hebben anderen meer voorbeelden en meer begeleiding nodig.



figuur 9 Ontwikkeling kernconcept

Leerlingen hebben aan de hand van deze contexten en de explicitering van het kernconcept in hun geheugen al een behoorlijk rijk schema van exponentiële groei in verschillende representaties (verbaal, grafisch, numeriek, algebraïsch) kunnen opbouwen. De aandacht verschuift in havo/vwo nu naar de kenmerken van de exponentiële functie en naar kunnen redeneren met die kennis en het vragen kunnen stellen en beantwoorden. Zo kunnen ze met behulp van VU-Grafiek uitzoeken wanneer twee verschillende groeiprocessen eenzelfde waarde voor een afhankelijke grootheid bereiken, zonder dat ze nog beschikken over algebraïsch gereedschap om die waarde te berekenen. Ook kunnen ze uit een beschrijving, een grafiek of een tabel opmaken welk exponentieel groeiproces in die context aan de orde is en daar een formule bij maken (*algebraïseren*), zonder dat ze een dergelijk model uit een differentiaalvergelijking kunnen opstellen. De *groeisnelheid* kunnen ze wel per tijdseenheid, hoe klein ook gekozen, benaderen, maar niet exact berekenen met de afgeleide functie. Het schema wordt rijker (***zie figuur 10***), terwijl het onderliggende concept van de exponentiële groei breder en tegelijk abstracter wordt. Die onderliggende abstractie geeft een steviger structuur aan het schema en maakt het ook mogelijk om in heel verschillende toegepaste en wiskundige situaties te herkennen dat er sprake is (of kan zijn) van een exponentieel verband.



figuur 10 Rijk en gestructureerd schema

Afhankelijk van het wiskundevak kan het schema nog verder groeien door verticaal mathematiseren (rijen, differentialen) of horizontaal mathematiseren (complexere echte toepassingen). Ervaringen met verschillende meer of minder geslaagde pogingen om de logaritme te formuleren in termen van een groeicontext laten zien dat er wellicht eerder sprake is van een nieuw schema dan van het opnemen in een bestaand schema.

Contexten als denkmodel voor het differentiëren

In de bovenbouw havo/vwo is de *start* van het differentiëren essentieel voor de opbouw van een schema dat rijk is aan betekenissen. Zie bijvoorbeeld het katern *De afgeleide in breder perspectief*[9] in het al eerder genoemde *Handboek Didactiek van de Wiskunde*.

Een goede context als denkmodel is bijvoorbeeld de val van een parachutist (***zie figuur 11***).



figuur 11 De parachutist

Een tabel van de hoogte boven de aarde is aanleiding tot allerlei vragen over de valsnelheid, de verandering van die snelheid, enzovoort. De grafische weergaven vormen de overgang naar weer andere contexten, waarin de snelheid waarmee de ene grootheid verandert ten opzicht van de andere kan worden onderzocht. Voordat er wordt gerekend, met de valkuil van rekentechnieken die het inzicht verduisteren, kan het *centrale concept* van de afgeleide in tabellen en grafieken al worden opgebouwd.
Rond dat concept bouwt zich dan geleidelijk een rijker schema op, analoog aan ***figuur 10***. Weer is het van belang dat de leerlingen door vragen, opgaven en toetsen steeds weer teruggebracht worden naar het centrale concept, dat de structuur en samenhang van het schema in hun langetermijngeheugen moet waarborgen.

6. Contexten om transfer te bevorderen

In de opbouw van het netwerk van begrippen en vaardigheden zijn in de fase van het verkennen en oefenen eenvoudige verhaaltjessommen ('contexten' met niet erg realistische situaties) opgenomen om leerlingen te leren hun wiskundige kennis te leren gebruiken in situaties die niet in wiskundige termen zijn geformuleerd. Het gaat bijvoorbeeld om het leren opstellen en interpreteren van vergelijkingen en formules bij situaties waarin grootheden een rol spelen. Dat helpt leerlingen bij het flexibel leren werken met het centrale concept *variabele* in plaats van de beperking tot algebraïsche vormen in x en y, zoals dat tot de jaren negentig van de vorige eeuw het geval was.
Tot aan het nieuwe programma van 1968 (de 'moderne wiskunde') bevatten de algebrahoofdstukken altijd een paragraaf met 'ingeklede vergelijkingen'. Dat waren niet-realistische verhaaltjessommen of puzzels die met behulp van het opstellen van een vergelijking konden worden opgelost. Voor het gros van de leerlingen was het onbegrijpelijk dat die opgaven iets te maken hadden met het gereken met letters, waar de algebra uit bestond. (Variabelen als representanten van grootheden vielen buiten hun algebraschema.) Buiten de wiskundelessen, bijvoorbeeld bij natuurkundige formules als $V = I \times R$, functioneerde die algebra dan ook niet. (Na 1968 verdween dat type opgave decennia lang helemaal, want toen ging het vooral om de formele en correcte wiskunde.)
Hoewel dit type niet-authentieke contexten wel een functie heeft bij het oefenen en verwerken, is er op veel van die 'verhaaltjes' terecht veel kritiek omdat ze de suggestie wekken uit de echte wereld te komen. In schoolboeken en nog erger in toetsen en examens blijken ze vaak eerder een zekere taalvaardigheid te toetsen dan een wiskundig begrip of een wiskundige methode. *Marieke: 'Opa, ik kan in die verhaaltjes de som niet vinden!'*

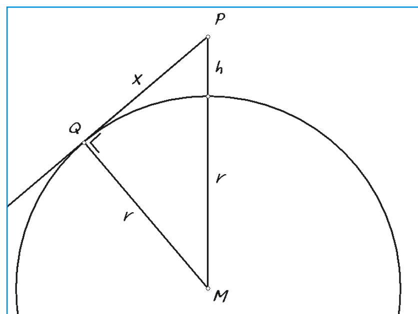
7. Contexten om (toegepaste) problemen op te lossen

In de geest van Polya[10] zou het moeten gaan om wiskundige en niet-wiskundige contexten, problemen die een beroep doen op een flexibele beheersing van de wiskundige begrippen en vaardigheden en op een goede probleemaanpak. Goede contexten zijn authentieke contexten, dus echt en realistisch, ontleend aan een werkelijkheid. Dankzij het verworven *wiskundig inzicht* is de leerling in staat om in analoge of nieuwe situaties (toegepast of wiskundig) de *toepasbaarheid* van het concept te herkennen en te benutten. Authentieke contexten kunnen afkomstig zijn uit de echte wereld of uit andere vakgebieden, zoals de economische, medische en technische wetenschappen en de natuurwetenschappen. Voor wiskunde B vormen de natuurwetenschappen en de techniek een waardevolle bron. Wegens de vreemde positie van wiskunde A in de profielen ligt het daar wat lastiger, omdat in de contexten niet veel kennis van en affiniteit met andere vakgebieden bekend kan worden verondersteld. Hetzelfde probleem doet zich voor in de sectoren van het vmbo. Authentieke contexten uit één bepaalde sector zijn natuurlijk heel motiverend, maar de wiskundelessen worden veelal aan leerlingen uit meerdere sectoren gegeven.

8. Contexten om te leren modelleren

Zoals de geciteerde wiskundigen in deel 3 van deze reeks al naar voren hebben gebracht, speelt de wiskunde een belangrijke rol in het *modelleren* van allerlei situaties en probleemstellingen. Zeker in de bovenbouw van havo/vwo is het van belang

dat leerlingen hiermee kennis maken, omdat het een kernactiviteit is van de gebruikers van wiskunde.



figuur 12 Horizonprobleem

We moeten daar nog wat meer werk van maken in relatief eenvoudige probleemstellingen. In het katern *Modelleren*[9] wordt aan de hand van voorbeelden besproken hoe daar in de bovenbouw havo/vwo meer werk van kan worden gemaakt. Het startprobleem (***zie figuur 12***) is de vraag: *Het is prachtig weer, je staat op het strand en kijkt naar de horizon. Hoe ver weg is die horizon?* Ook bij het modelleren is een systematische probleemaanpak noodzakelijk om de gegeven situatie adequaat door een wiskundig model te kunnen beschrijven en vervolgens dat model te evalueren.

9. Een instructiemodel

In de loop van de tijd zijn verschillende instructiemodellen ontworpen die beter dan het VNO-model (*voordoen*, *nadoen*, *oefenen*) leerlingen helpen een rijk schema van begrippen en routines te ontwikkelen; zie Katern 0 van het *Handboek Didactiek van de Wiskunde*[9]. Op grond van de hiervoor weergegeven analyse kan het ***in het kader*** geplaatste instructiemodel wiskundeleraren helpen hun eigen onderwijs te evalueren en te verbeteren.

INSTAP - Samen werken aan een rijke context dat als denkmodel kan dienen voor het op te bouwen schema in het langetermijngeheugen.

Onderwijsvorm	Klassengesprek, afgewisseld met werken in tweetallen/groepjes.
Docent(e)	Context aandragen, probleem stellen.
Leerlingen	Ideeën opperen, bespreken, reflecteren.
Doel	Oriënteren op kernbegrip en typen problemen.

OPSTAP - Eenvoudige toegepaste en wiskundige situaties aan de hand waarvan leerlingen op het spoor komen van de kenmerken van de begrippen, technieken en abstracties waarom het in dit gebied gaat.

Onderwijsvorm	Zelfstandig werken in tweetallen/groepjes.
Docent(e)	Stevig controleren, bijsturen, soms klassikaal nalopen.
Leerlingen	Opgaven maken, kenmerken opsporen, zelfcontrole.
Doel	Kenmerken van begrippen en technieken opsporen.

EXPLICITEREN - Op basis van de gemaakte opgaven en observaties samen onder woorden brengen wat de kenmerken van de begrippen, methoden en technieken zijn, de kern van het schema.

ONDERWEG - Opbouw in combinaties van de begrippen en technieken aan de hand van meer complexe situaties en verbindingen met al eerder verworven kennis.

Onderwijsvorm	Zelfstandig doorwerken in tweetallen/groepjes/individueel.
Docent(e)	Terughoudend begeleiden, algemene hints.
Leerlingen	Opgaven maken, zelfcontrole.
Doel	Verder ontwikkelen van het schema met begrippen en technieken.

WEGWIJZERS - Momenten van terugkoppeling en reflectie naar aanleiding van kernopgaven.

Onderwijsvorm	Klassikaal leergesprek.
Docent(e)	Vragen oproepen, doorvragen, verwoorden, samenvatten.
Leerlingen	Mondeling vragen beantwoorden, meedenken, schriftelijk vastleggen.
Doel	Expliciteren, leren over wat je hebt geleerd.

CONTROLEPOST - Diagnostische toetsing, leren van eigen werk.

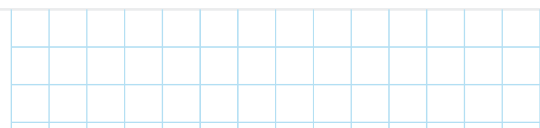
Onderwijsvorm	Mondeling individueel, klassikaal schriftelijk.
Docent(e)	Terugkoppelen, doorverwijzen, reconstrueren.
Leerlingen	Vragen beantwoorden, opgaven maken, conclusies over eigen werk vastleggen.
Doel	Consolideren/monitoren beheersing van begrippen/technieken.

VERWERKING - Toepassing op complexere situaties, authentieke contexten, expliciteren probleemaanpak.

Onderwijsvorm	Zelfstandig werken, afgewisseld met klassikale reflectie.
Docent(e)	Stimulerend begeleiden, klassikaal reflecteren.
Leerlingen	Probleem oplossen, terugkijken.
Doel	Transfer van basiskennis, leren probleem oplossen.

INTEGRATIE - Overzicht van begrippen, technieken en methoden in relatie tot typerende problemen en contexten. Verbinding leggen met andere kennis en situaties.

Onderwijsvorm	Zelfstandig, afgewisseld met klassikale reflectie.
Docent(e)	Stimulerend begeleiden, klassikaal reflecteren.
Leerlingen	Probleem oplossen, terugkijken.
Doel	Integratie van nieuwe kennis en koppelen aan al bestaand kennisschema.



10. Wat werkt wel/niet en waarom dan?

Dankzij de wetenschappelijke kennis over informatieverwerking en de rol van de kennisschema's van ons langetermijngeheugen begrijpen we beter waarom iets niet werkt. We begrijpen dat een didactiek van Voordoen-Nadoen-Oefenen niet leidt tot een blijvende leeropbrengst, omdat dat die routines los worden opgeslagen en na een tijdje niet meer adequaat kunnen worden opgeroepen. We begrijpen dat een opsplitsing van de leerstof in kleine deelgebieden, die los van elkaar worden onderwezen, leidt tot ad-hoc-succes op dat moment maar niet tot samenhangend kennis. We begrijpen nu dat leerlingen wel een vergelijking sec kunnen oplossen, maar het verband met een grafiek niet zien. We begrijpen dat leerlingen vergelijkingen kunnen oplossen, maar geen idee hebben wat ze doen en hoe ze hun oplossing kunnen controleren, omdat het onderliggend concept van een vergelijking niet centraal staat in hun schema. We begrijpen dat leerlingen een functie met rekenregels kunnen differentiëren zonder dat ze een relatie met de snelheid in natuurkunde of de helling van een grafiek kunnen leggen. We begrijpen dat het schier onmogelijk is om de goniometrische verhoudingen in een driehoek te koppelen aan de goniometrische functies, omdat ze tot totaal verschillende schema's behoren. We begrijpen nu dat leerlingen niet zonder een door ons vooraf bedachte leerweg zelf een adequaat schema kunnen opbouwen, omdat zij niet kunnen weten welke kernconcepten op de duur centraal moeten staan. Kortom, als we denken in termen van betekenisrijke schema's begrijpen we beter waarom iets niet werkt of altijd weer, jaar op jaar, fout gaat.

Begrijpen waarom iets in het onderwijs niet goed werkt, is het begin van een ontwerp om ons onderwijs beter, meer succesvol, bevredigender, te doen verlopen. Met de besproken 'theorie' in het achterhoofd begint het creatieve werk om een onderwerp, hoofdstuk, lange leerlijn eens opnieuw te doordenken en een nieuw ontwerp te maken.

Is dat niet de uitdaging van ons beroep als wiskundeleraar?

Verwijzingen

[1] De delen 1, 2 en 3 zijn verschenen in *Euclides* 83(8), 84(3) en 84(5).

[2] Zie *www.minocw.nl/documenten/4322.pdf* of *www.slo.nl*.
- Eindrapport Expertgroep: *Over de drempels met taal en rekenen*. SLO 2008.
- Deelrapport rekenen&wiskunde: *Over de drempels met rekenen*. SLO 2008.

[3] cTWO (2008): *Verkennen, gebruiken, verdiepen*. Rapport programmacommissie onderbouw havo/vwo (website: *www.ctwo.nl*).

[4] R. Skemp (1978): *Inzicht, planning en het bijbrengen van routine*. In: *Euclides* 53(9).

[5] J. van Dormolen (1974): *Didactiek van de wiskunde*. Utrecht: Oosthoek's Uitgeversmaatschappij BV. (1976: Scheltema & Holkema BV).

[6] J.D. Bransford, A.L. Brown, R.C. Cocking, editors (2000): *How People Learn*. Washington D.C.: National Academy Press.

[7] K. Kilpatrick, J. Swafford, B. Findell, editors (2001): *Adding it Up. Helping Children Learn Mathematics*. Washington D.C.: National Academy Press.

[8] W.J. Bos (1984): *Gebruik je hersens!* In: W.J. Bos, P.M. van Hiele, L. Streefland, A. van Streun: *Wiskundige problemen en toepassingen*. Groningen: RUG, Mathematisch Instituut.

[9] ELWIeR: *Handboek Didactiek van de Wiskunde*. Zie *www.elwier.nl* (materiaal); onder andere: *Katern 0: Leren en Onderwijzen van Wiskunde, Katern 1: Vergelijkingen vergelijken, Katern 2: De afgeleide in breed perspectief, Katern 3: Modelleren.*
ELWIeR = Expertisecentrum Lerarenopleiding Wiskunde en Rekenen.

[10] - G. Polya (1945): *How to solve it*. Princeton (NJ): Princeton University Press.
- G. Polya (1962): *Mathematical Discovery I*. New York: Wiley and Sons.
- G. Polya (1965): *Mathematical Discovery II*. New York: Wiley and Sons.

Over de auteur

Anne van Streun was voorzitter van de werkgroep rekenen & wiskunde van de Expertgroep Doorlopende Leerlijnen Taal en Rekenen.
E-mailadres: *avstreun@euronet.nl*

Wiskundeonderwijs in de dagelijkse praktijk

OP BEZOEK BIJ HET ICHTHUS COLLEGE IN VEENENDAAL

[Klaske Blom]



Herman van Ravestein en Nico van Houwelingen

De vakgroep wiskunde van het Ichthus

De sectie wiskunde van het Ichthus bestaat uit 15 personen en met twee ervan spreek ik vandaag. Het zijn Nico van Houwelingen en Herman van Ravestein, beiden volgens eigen zeggen nog nieuwelingen in het vak en met hun hoofdtaak binnen het vmbo. Herman is bezig aan zijn tweede jaar als docent, maar hij kent de school op zijn duimpje omdat hij er ook als leerling al jaren doorbracht. Nico vindt zichzelf nog beginnend – in mijn oren klinkt hij behoorlijk ervaren; na zes jaren ga je voor je het weet bij de 'oude rotten' horen.
Breed sectieoverleg is er 4 à 5 keer per jaar en daarnaast spreken collega's die in eenzelfde leerjaar werken elkaar vaker informeel in de wandelgangen en pauzes. Nico licht dit toe: *Elk leerjaar heeft een coördinator die voor zijn/haar leerjaar de planning maakt voor het hele jaar: in het vakwerkplan zijn voor het hele jaar alle weken ingevuld wat betreft toetsen en so's. Ook per les is het programma bijna helemaal vastgelegd zodat iedereen zich zoveel mogelijk aan dezelfde planning houdt. Dat schept duidelijkheid voor leerlingen en ook voor nieuwe collega's. Het helpt bij de voorbereidingen. Ja, en natuurlijk zijn er wel collega's die deze planning een te strak keurslijf vinden en die afwijken van de afspraak, maar dat is geen probleem.*
Een mooie traditie moet worden dat er tijdens het gezamenlijke sectieoverleg altijd een didactische vraag op de agenda staat. Bijvoorbeeld 'Hoe lossen we vergelijkingen op in klas 2, 3 of 4; wat is de aanpak?' of 'Hoe leid jij een dit nieuwe hoofdstuk in?' Er worden ervaringen uitgewisseld en er wordt van elkaar geleerd. Vooral ook op het gebied van 'een goede notatie' zijn de sectiegenoten met elkaar in gesprek.

Profiel van de school

Het Ichthus college is een 'witte' en christelijke school. 99% van de leerlingen is van kerkelijke afkomst, hoewel dit percentage terug lijkt te lopen omdat ook niet-kerkelijke ouders kiezen voor de school vanwege de normen en waarden die er gehanteerd worden. Nico en Herman zijn het er over eens: *We zouden onszelf typeren als traditioneel, met conservatief onderwijs waarbij vooral frontaal gewerkt wordt. Er worden wel experimenten gedaan zoals Taaldorp, maar dat is niet de hoofdmoot van ons werk.*
Er is een bèta- en een gymnasiumstroom op school waar leerlingen minder uren per vak investeren (omdat ze het in minder tijd aankunnen) en de vrijgekomen tijd besteed kan worden aan extra projectonderwijs. Binnen het vmbo kan het vak technologie en/of lichamelijke oefening 2 gevolgd worden. Technologie is een verplicht vak in klas t3 en een keuzevak in klas t4, maar alleen als extra vak.
Wiskunde heeft binnen het Ichthus een determinerende functie. Sinds schooljaar 2007-2008 krijgen leerlingen twee gemiddelden, het A-gemiddelde voor alle vakken, en het S-gemiddelde voor een selectie van vier vakken waarvan ook wiskunde deel uitmaakt. Voor de overgang en ook voor 'opstromers' is het S-gemiddelde van belang.

De wiskundedocent aan het werk

Herman heeft een uitgesproken mening, zijn hart ligt bij tweedeklassers vmbo: *Het leeft in zo'n klas. De kinderen komen binnen en moeten eerst even kletsen, vertellen waar ze mee bezig zijn. Het is belangrijk dat ze respons krijgen en het gevoel hebben dat ik met ze mee leef en in hun persoon geïnteresseerd ben. Ik moet eerst contact maken; het hoeft maar 'effe' aan het begin van de les en daarna gaan we aan het werk.*
Nico: *Dat moet je op havo en vwo ook doen, hoewel je daar toch meer leerlingen er tussen hebt zitten die uit zichzelf aan het werk gaan en dat sociale contact niet zo nodig lijken te hebben. Ik geef volgens mij niet zo veel*

anders les in een vwo- dan in een vmbo-klas. Misschien ben ik wel te veel dictator, ik zeg gewoon dat we het zo en zo gaan doen.
Vooral in het vmbo moet het klikken tussen docent en leerling want vmbo-leerlingen werken voor de docent. Ze zeggen het ook: 'Je denkt toch zeker niet dat ik voor die vent iets doe?'. Herman vat het nog eens samen: *Interesse hebben in de wereld van je leerlingen en streng zijn in het begin, structuur bieden, daar gaat het om.* Daarnaast heeft hij het idee dat de vragen als 'dat snap ik niet', 'ik snap er niets van' veelvuldig en snel klinken in t2-klassen. Nico filosofeert er over door: *Vmbo-ers voelen zich vaak het laagste niveau op school en dat is niet goed voor hun zelfvertrouwen. Dat komt door onze school: hier vormen ze ook het laagste niveau, terwijl dezelfde leerlingen, als ze op een school zouden zitten met kader- en beroepsleerlingen, zich misschien beter zouden voelen. Maar ouders willen graag dat hun kinderen bij ons blijven vanwege de identiteit van de school, ook al is het niveau misschien soms te hoog voor ze.*

De specialiteiten van het wiskunde-onderwijs op het Ichthus

1. Wedstrijden

Een van de leuke activiteiten in het onderwijs is dat er op het Ichthus altijd meegedaan wordt met de Kangoeroe-wedstrijd en met de Wiskunde Olympiades; in de bètastroom zelfs verplicht.

2. Rekenonderwijs

Sinds een paar jaar is er extra aandacht voor hoofdrekenen in de tweede klassen omdat ervaren collega's zagen dat de reken-vaardigheden van leerlingen echt achteruit gingen en, omdat er o.a. in de boven-bouw gaten vallen, leerlingen te weinig basisvaardigheden en -kennis hebben. Dit werd bevestigd door de vele berichten in de media over de slechte rekenkwaliteit.
Herman: *Wij hebben zelf een rekenboekje gemaakt, eigenlijk voor 2hv en het daarna aangepast voor 2t. Het is echt weer ouderwets hoor: staartdelingen, breukrekenen. We leren ze weer rekenen op onze eigen manier, dus niet met herhaald aftrekken als het om delen gaat.*
Nico gaat in op het belang van een goed getalbegrip: *We vinden het belangrijk dat leerlingen weer getalbegrip ontwikkelen, want dat herhaald aftrekken gaat bijvoorbeeld fout met kommagetallen. De omweg die ze maken met herhaald aftrekken is te groot, het kan veel praktischer. We leren leerlingen een paar belangrijke zaken aan en verder moeten ze oefenen, oefenen, en ermee bezig zijn.*
In de loop van het jaar krijgen leerlingen ook rekentoetsen die meewegen in hun wiskundecijfer. Rekenen heeft dus een groot gewicht gekregen op het Ichthus. Niet alleen door de extra rekenlessen in de tweede klas, maar ook door, bij de behandeling van sommige hoofdstukken in de brugklas, af te zien van gebruik van de rekenmachine. Het ligt op langere termijn in de bedoeling dat er gedurende de hele schoolcarrière aandacht aan besteed wordt. *We willen het rekenen uit de bovenbouw weghalen; als ze naar de bovenbouw gaan, moeten ze rekenvaardigheden paraat hebben. Dan kunnen we tenminste aan de wiskunde toekomen.* Nico wil nog iets nuanceren. Hij onderkent het probleem met de rekenvaar-digheden, maar heeft soms ook leerlingen van wie hij liever wil dat ze met de machine leren werken dan dat ze gaan hoofdrekenen omdat dat waarschijnlijk nooit tot iets goeds zal leiden. *Sommige kinderen zijn zo zwak dat ze het echt niet gaan begrijpen. Als je het al vijf keer, en ook op verschillende manieren geprobeerd hebt, blijft er soms niets over dan voor- en nadoen. Dan zeg ik liever: Doe het gewoon zo op de rekenmachine. Worstel je door de wiskunde heen nu het nog verplicht is en als er een kans is om het te laten vallen, doen!*

Praktische opdracht

In de vierde klassen vmbo-t wordt al enige jaren eenzelfde praktische opdracht (Inrichten van een nieuwe slaapkamer; ***zie figuur 1*** en ***figuur 2***) gegeven, omdat deze goed bevalt. Nico: *Leerlingen krijgen een plattegrond van een huis: dit wordt jouw huis en dit wordt jouw kamer. Er zit een raam in, er zit een deur in. Je moet er vloerbedekking in leggen en je moet gordijnen ophangen en behangen. Daar krijg je een budget van € 400 voor. En vervolgens moet de kamer ingericht worden voor € 1200. Er moet een bed in – met alles er op en er aan – er moet*

De Taak

De slaapkamer ga je eerst opknappen: een nieuw fris behangetjes tegen de muren, nieuwe vloerbedekking en gordijnen.





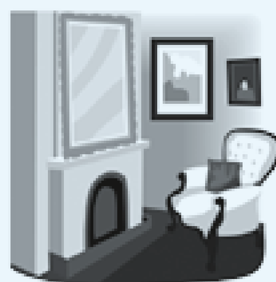
Daarna mag je de kamer nieuw inrichten. Je hebt in ieder geval een bed nodig met toebehoren (matras, kussen, dekbed enz.), een bureau met stoel en een hang-legkast. Ook heb je verlichting nodig.

Voor de opknapbeurt heb je een budget van € 400,=
Voor de inrichting heb je een budget van € 1200,=
Wat je overhoudt van het budget mag je besteden aan accessoires (leuke dingetjes)

Het volgende is wel van belang: alles wat je koopt , moet nieuw zijn. Je mag dus geen spullen kopen op Marktplaats of via "gratis af te halen" sites.

Je maakt van deze opknapbeurt en inrichting een werkstuk. Er wordt gewerkt in groepjes van 3 à 4 personen.

Bij dit werkstuk zitten 2 bijlagen. Deze moeten je helpen om niets te vergeten en laten je zien hoe je op een nette manier je gegevens kan ordenen. Je mag deze bijlagen gebruiken, maar je kunt ook zelf iets soortgelijks maken. Zorg in ieder geval dat je alle vragen beantwoord. Denk hierbij aan eventuele berekeningen.



figuur 1 Pagina 3 uit de praktische opdracht

Stap 2: Informatie verwerken

Knap slaapkamer 2 op, doe dit aan de hand van de vragen.

Behang:

Maak de volgende opdrachten. Laat m.b.v. berekeningen zien hoe je aan je antwoord bent gekomen.



1. Reken uit hoeveel banen behang je nodig hebt, neem 2 banen extra voor het geval er iets misgaat.
2. Reken vervolgens uit hoeveel rollen behang je nodig hebt.
3. Bereken het bedrag wat je kwijt bent aan rollen behang.
4. Om te kunnen behangen heb je ook lijm en gereedschap nodig.
   Ga er globaal vanuit dat dit ongeveer 30% is van de kosten voor het behang.
   Bereken hoeveel je kwijt bent voor lijm en gereedschap.
5. Hoeveel kost het behangen in totaal? Vul dit in antwoord in op **bijlage 2**.

Vloerbedekking

Maak de volgende opdrachten. Laat m.b.v. berekeningen zien hoe je aan je antwoord bent gekomen.

1. Ga na hoeveel meter vloerbedekking je nodig hebt.
   Houdt er rekening mee dat je iets meer vloerbedekking moet kopen i.v.m. snijverlies. Neem hiervoor 15 cm extra.
2. Bereken het bedrag wat je kwijt bent aan vloerbedekking.
3. Om vloerbedekking te kunnen leggen heb je ook lijm nodig.
   Je hebt 500 gram lijm nodig per m².
   Hoeveel gram lijm heb je nodig?
4. De lijm wordt verkocht in emmers van 1 kg en 3 kg.
   Een emmer van 1 kg kost € 4,69 en een emmer van 3 kg kost € 9,99.
   Welke emmers kun je het beste kopen?
5. Hoeveel kost de lijm in totaal?
6. Wat kosten de vloerbedekking en de lijm bij elkaar? Vul dit antwoord in op **bijlage 2**.



figuur 2 Pagina 5 uit de praktische opdracht

een hang/legkast in en een bureau en een stoel. Aan het eind heb je budget over, dat is voor de accessoires. Leerlingen moeten dus een plattegrond en een kostenplaatje maken. En dit is nog knap lastig vanwege bijvoorbeeld de afmetingen van behangstroken.

Er was vast nog meer te bespreken, maar er moest na een klein uurtje weer gewerkt worden: de leerlingen wachtten.
Nico en Herman hartelijk dank voor het gesprek!

Over de auteur
Klaske Blom is hoofdredacteur van *Euclides* en als wiskundedocent werkzaam op 't Hooghe Landt in Amersfoort.
E-mailadres: *klaskeblom@gmail.com*

De staartdeling is nooit weg geweest

[Lonneke Boels]

Staartdeling als symbool

Met enige regelmaat duikt in de media de discussie over de staartdeling op. Kinderen zouden deze niet meer leren en dat zou één van de verklaringen zijn voor de tegenvallende resultaten voor rekenen bij leerlingen. De staartdeling is daarmee symbool geworden voor algoritmen die niet meer worden aangeleerd en voor de daaruit voortvloeiende problemen.
In dit artikel zal ik laten zien dat de notatie van de staartdeling weliswaar anders is, maar dat het algoritme dat de kinderen wordt aangeleerd, nog steeds hetzelfde is. Het is zelfs vrij eenvoudig om van de ene notatie naar de andere te gaan, zoals ik ook met voorbeelden zal laten zien.

In het rapport *Doorlopende Leerlijnen Rekenen* [7] wordt aangegeven dat onder andere bij het delen de resultaten significant achteruit zijn gegaan. Een mogelijke verklaring voor de oorzaak wordt ook al gegeven: leerlingen noteren hun berekeningen niet, maar proberen alles uit hun hoofd uit te rekenen.
Dat is waarschijnlijk een betere verklaring voor de problemen met delen dan het idee dat het aan het (niet) aanleren van de staartdeling zou liggen. Dit vermoeden wordt verder onderbouwd door het gegeven dat de zwakkere rekenaars in het Nederlandse rekenonderwijs relatief beter presteren dan in andere landen.

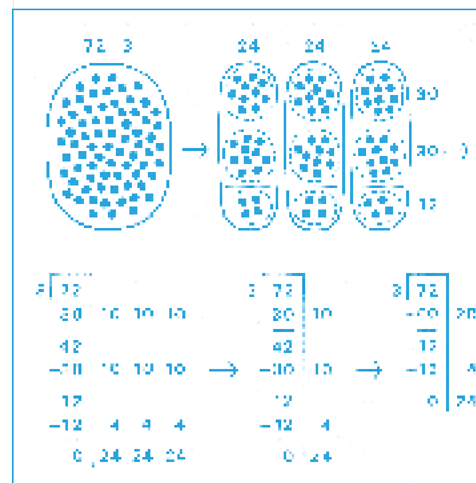
Het aanleren van het delen

Hoe gaat tegenwoordig het aanleren van de staartdeling? Dit aanleren gaat in verschillende stappen. In de kleuterklassen (groep 1 en 2) begint het leren delen eigenlijk al. Een kind is jarig en gaat de traktatie, bijvoorbeeld op zelfgebakken koekjes, eerlijk verdelen. Bij dit delen krijgt iedereen eerst één koekje en als er genoeg over is, krijgen de kinderen er weer één. Dit gaat net zo lang door totdat er niet meer genoeg over is om iedereen één koekje te geven. In groep 3 wordt hier op voortgebouwd door appels, kastanjes, steentjes, geld enz. eerlijk te verdelen; ***zie figuur 1***. De vraag 'Hoe heb je verdeeld?' wordt klassikaal besproken en



figuur 1 Voorbeeld van leren delen uit RekenRijk, een rekenmethode voor groep 3[1]

hierbij wordt dan een eerste stap gemaakt naar het noteren en formaliseren: het verticale mathematiseren. In plaats van verdelen over kinderen wordt nu soms ook verdelen over kommetjes gebruikt: ook een eerste abstractie. In de loop van de volgende jaren wordt deze methode genoteerd en steeds verder geformaliseerd; zie de voorbeelden ***in figuur 2*** en ***in figuur 3***.
Zoals u ziet, begint het met herhaald aftrekken van hoeveelheden die de leerling zelf kiest. Er wordt wel gestreefd naar handige veelvouden (bijvoorbeeld 10 tegelijk). Daarbij wordt vaak gebruik gemaakt van een tabel met hulpsommen zoals in het voorbeeld hierna.

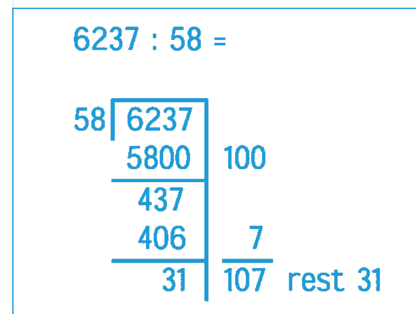


figuur 2 Voorbeeld van stappen in het proces van aanleren van het deelalgoritme middels herhaald aftrekken in een didactiekboek voor de Pabo[2]

Delen	uitgebreid		verkort	
1976 : 52	1976		1976	
	1040	20x	1560	30x
	936		416	
	520	10x	416	8x
	416		0	
	208	4x		
	208			
	208	4x		
	0			

figuur 3 De laatste twee stappen in het aanleren van het algoritme van het delen zoals de uitgever van de rekenmethode Pluspunt dit uitlegt aan leerkrachten en ouders[3]

De bedoeling is dat de toekomstige leerlingen van havo en vwo uiteindelijk de kortste manier van dit algoritme gebruiken. Dat ziet er dan bijvoorbeeld als volgt uit als ***in figuur 4***.
Daarbij wordt gebruik gemaakt van een hulptabel die er als volgt kan uitzien:
1 × 58 = 59
2 × 58 = 116
4 × 58 = 232
5 × 58 = 290
10 × 58 = 580
7 × 58 = 406



figuur 4 Kortste notatie van een deling in de rekenboeken die op basisscholen worden gebruikt

6237 : 58 =

A

```
58 | 6237 |
     5800 |  100
     ----
      437 |
      406 |  7
     ----
       31 |
       29 |  0,5
     ----
        2 |
     1,74 |  0,03
     ----   ------
     0,26 |  107,53 rest 0,26
```

B

```
58 / 6237 \ 107,53
     58
      437
      406
       310
       290
        200
        174
         26
```

figuur 5 Deling volgens nieuwe notatie (A) en diezelfde deling met een staartdeling (B)

De traditionele manier van oplossen van de staartdeling leidde in het hierboven gegeven voorbeeld steevast tot problemen. Veel leerlingen gaven hier als antwoord: 17 door het vergeten van de 'nul' (***zie figuur 5B***). Deze problemen waren nog groter als er ook cijfers na de komma moesten worden gegeven. De komma werd vaak verkeerd geplaatst met grote gevolgen voor de uitkomst. Als we de twee notaties naast elkaar zetten, wordt duidelijk waarom de kans op fouten bij de nieuwe notatie minder groot is: er wordt met de correcte cijfers gerekend en niet met losse getallen; ***zie figuur 5A***, ***figuur 5B*** en ***figuur 7***.
Bij de berekening in figuur 5A kan een hulptabel als onderstaand worden gebruikt:
0,1 × 58 = 5,8
0,5 × 58 = 29
0,01 × 58 = 0,58
0,02 × 58 = 1,16
0,03 × 58 = 1,74

Het delen vroeger

Maaike zat aan haar bureautje huiswerk te maken. Ze keek hem stralend aan, want ze was net bezig met staartdelingen en ze wist dat Tjerk daar heel goed in was. 'Kom je me helpen?', vroeg ze. Tjerk pakte een stoel, ging naast haar zitten en keek naar de ellenlange som. 'Hij komt niet uit', zuchtte ze. 'Ik word er gek van. Ik zit al een half uur op die rotsom.' [5]

Destijds leverde het direct aanleren van de staartdeling een groot aantal problemen op die door sommigen nu vergeten lijken, zoals ik onlangs nog kon constateren. Een leerling uit groep 7/8 was aan het worstelen met de staartdeling. Zijn leerkracht had hem het trucje geleerd, maar het was duidelijk dat hij er niets van begreep. Hij moest twee kommagetallen op elkaar delen en schoof maar wat met de komma's. Na een kwartier was hij nog nauwelijks verder. Een vmbo-docent die als basisschoolleerkracht zo'n 40 jaar geleden is begonnen en daarna jaren op een huishoudschool en later vmbo heeft gewerkt, bevestigde eveneens dat er een grote groep leerlingen was die de staartdeling niet onder de knie kreeg. Van enig inzicht door herhaalde oefening was hierbij geen sprake.
Ook de uitgever van de rekenmethode *Pluspunt*[3] somt een aantal nadelen van het oude leerproces op. De meest voorkomende problemen met de staartdeling waren:

- zwakke rekenaars kregen het algoritme meestal niet onder de knie;
- zwakke rekenaars hadden geen alternatieve strategie als de staartdeling niet lukte;
- als het antwoord een '0' bevatte, werd deze nogal eens vergeten waardoor het antwoord ongeveer een factor 10 (of 100 of …) te klein was;
- voor delingen met kommagetallen moesten de leerlingen aparte regels leren; hiermee werden veel fouten gemaakt, met name ook weer door de zwakke rekenaars.

Pluspunt: Wat zijn de verschillen met vroeger? Als u kijkt naar [de] voorbeelden, dan ziet u verschillen bij vermenigvuldigen en vooral bij delen. Vroeger, bij het ouderwetse 'cijferen', werd een getal opgesplitst in de verschillende cijfers en daar moest je dan volgens vaste regels mee werken. Dat leidde tot trucjes met nullen en open plaatsen. Sommige kinderen werden daarin heel handig door veel te oefenen zonder dat ze een idee hadden wat ze precies aan het doen waren.
Kinderen noteren bij het huidige rekenen hun berekeningen uitgebreider, zeker in het begin. Dat komt omdat de kinderen steeds met een heel getal werken. Ze realiseren zich dat de '5' uit 53 staat voor 50 en met dat getal gaan ze rekenen. De verschillen tussen vroeger en nu zijn echter ook weer niet zo erg groot. De verkorte vorm van nu lijkt erg veel op de ouderwetse manier. De kinderen nu doen iets meer schrijfwerk, hebben daardoor meer inzicht en minder kans op fouten! [3]

Staartdeling als kortste notatie

Dankzij de discussie over het rekenen staat de staartdeling nu weer in sommige wiskundeboeken, zoals in *Getal en Ruimte*. Wat ik daarbij een gemiste kans vind, is dat er niet even een link wordt gelegd met de aangeleerde notatievorm. De staartdeling kan dan wat mij betreft gepresenteerd worden als de kortste notatievorm en is dus een logische volgende stap in het proces van delen als herhaald aftrekken. In een didactiekboek over het rekenonderwijs[4] vond ik een prachtig voorbeeld over precies deze overgang; ***zie figuur 6***.
Want laten we wel wezen, de staartdeling heeft voor rekenaars één groot voordeel: door de overbodige cijfers tijdelijk weg te laten blijven de vermenigvuldigingen beperkt tot kleine(re) getallen. Het is niet voor niets dat Van de Craats in zijn artikel[6] schrijft '… en is de staartdeling niet gewoon de meest efficiënte hapmethode?'
De 'hapmethode' is een benaming voor deze 'nieuwe' manier van delen via herhaald aftrekken. In de nieuwe boeken van *Moderne Wiskunde* voor de brugklas van havo en vwo wordt bijvoorbeeld wel teruggegrepen naar de 'hapmethode', alleen wordt hier de staartdeling (nog) niet aangeleerd of herhaald.

Overigens, er wordt door tegenstanders van de ‘nieuwe’ rekenmethoden hard geroepen dat ze niet goed zijn (o.a. kolomsgewijs rekenen), omdat het van links naar rechts is terwijl ‘alle andere’ methoden voor het cijferen van rechts naar links zijn. Maar mij valt op dat ook deze staartdeling van links naar rechts is…

Door de zwakke rekenaars de strategie van herhaald aftrekken met kleinere happen te leren en vervolgens de (toekomstige) havo/vwo-leerlingen de staartdeling te leren als de ultieme verkorting van deze methode, combineren we in mijn ogen het beste van twee werelden. Het biedt bovendien het voordeel dat de staartdeling verderop in de opleiding met letters kan worden uitgevoerd, hetgeen bij de exacte hbo- en wo-opleidingen nogal eens vereist is. Overigens kunnen dergelijke vraagstukken ook zonder de staartdeling worden opgelost, maar dat terzijde.

Als dan bovendien het verband wordt gelegd tussen de ‘hapmethode’ en de staartdeling, wordt tegelijk tegemoet gekomen aan één van de kritiekpunten van de commissie Dijsselbloem op het wiskundeonderwijs. Er wordt dan immers wél voortgebouwd op de kennis en methoden die leerlingen op de basisschool hebben geleerd. En daar zijn onze leerlingen nog het meest bij gebaat.

Er woedt een rekenoorlog lijkt het wel. Je bent óf voor Van de Craats c.s. (en dus tegen Freudenthal c.s.) óf tegen. Persoonlijk vind ik dat jammer. Want volgens mij willen alle docenten die zich hierover druk maken, uiteindelijk hetzelfde: dat onze leerlingen *goed* kunnen rekenen. Dat lukt alleen als wij genuanceerd kijken naar wat werkt en wat niet, én onze vooringenomenheid durven te laten varen.

figuur 6 Overgang van herhaald aftrekken naar staartdeling[4]

figuur 7 Voorbeeld van herhaald aftrekken (verkorte methode)[4]

Noten

[1] *RekenRijk, leerlingenboek voor groep 3*. Groningen: Wolters-Noordhoff (2e editie).

[2] F. Goffree (1992): *Wiskunde en didactiek, deel 2*. Groningen: Wolters-Noordhoff (2e druk).

[3] Zie: *www.malmberg.nl/systeem/images/rekenresultaten-Pluspunt_tcm6-32767.pdf*

[4] K. van Broekhuizen e.a. (1994): *Rekenen in beweging*. Uitgeverij SLO/VPC (ISBN 9062387004).

[5] J. Vriens (1984): *De zesde tegen het soepie*. Houten: Van Holkema en Warendorf.

[6] T. Braams, M. Milikowski (redactie): *De gelukkige rekenklas*. Amsterdam: Uitgeverij Boom; pag. 34 (ISBN 978-90-8506-615-6).

[7] Expertgroep Doorlopende Leerlijnen (2008): *Over de drempels met rekenen*. Deelrapport van de Eindrapportage van de Expertgroep Doorlopende Leerlijnen Taal en Rekenen. Zie: *www.taalenrekenen.nl/Algemeen/Nieuws/00002/Rekenrapport.pdf*

Over de auteur

Lonneke Boels is wiskundedocente op het Christelijk Lyceum Delft. Daarnaast heeft zij invalwerk verricht op een basisschool en op een Pabo. Zij heeft haar eigen bedrijf, Alaka (*www.alaka.nl*), waarin zij onder andere materialen maakt voor een Pabo voor de nascholing van basisschoolleerkrachten en wiskundebijlessen geeft. Zij is bovendien een van de ontwikkelaars van de rekenlessen voor de bovenbouw havo binnen een project van de NVvW.
E-mailadres: *L.Boels@alaka.nl*

Zwakke sleutels bij het RSA-cryptosysteem

DEEL 1

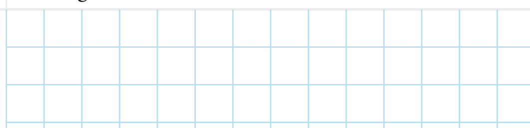
[Benne de Weger]

1. Inleiding

In het nieuwe vak Wiskunde D is er, gelukkig, aandacht mogelijk voor cryptografie als een leuke en veelgebruikte toepassing van wiskunde. Daarbij kan goed gekozen worden voor het behandelen van het RSA-cryptosysteem (zie paragraaf 3 voor de herkomst van de afkorting RSA). Een tekst over cryptografie voor gebruik bij Wiskunde D die dit doet, is [1; Lambeck].
Aantrekkelijke aspecten van RSA zijn dat de wiskundige basis ervan goed te begrijpen is voor leerlingen in de bovenbouw van het vwo, en dat de wiskunde die er bij komt kijken, niet de standaardwiskunde uit de hoek van de analyse of de statistiek is. Zo krijgen de leerlingen een goede illustratie van de breedheid en de toepasbaarheid van de wiskunde. Daarnaast laat het leerlingen kennismaken met een actief onderzoeksgebied in de wiskunde, dat ook andere disciplines raakt, zoals informatica.
Bij het behandelen van RSA kan goed uitgelegd worden hoe elementaire getaltheorie een cruciale rol speelt in moderne technieken voor beveiliging van informatie, zoals vertrouwelijkheid (versleuteling) en authenticatie (digitale handtekeningen).
Onderwijsteksten waarin de basisideeën van RSA worden uitgelegd komen echter nogal eens niet verder dan te vertellen hoe een sleutelpaar in elkaar zit, welke rol het ontbinden in factoren speelt bij het kraken van de sleutel, en hoe de RSA-operaties in hun werk gaan. Dat is wel te begrijpen, want die aspecten van het onderwerp hebben al een redelijke omvang, geven een aardig beeld van moderne cryptografie, en er valt al genoeg plezier aan te beleven.
In dit artikel, verdeeld in twee delen, willen we een minder bekend aspect van RSA wat verder uitdiepen: het bestaan van zogeheten *zwakke sleutels*. Dat zijn sleutels die vermeden moeten worden, omdat het gebruik ervan leidt tot het uitlekken van de geheime sleutel. Dit is een actief onderzoeksgebied in de wiskundige cryptologie. Enkele basisresultaten hieruit vereisen alleen elementaire getaltheoretische voorkennis, en die zullen we bespreken. Het doel daarvan is de docent die RSA wil behandelen, wat meer achtergrond te geven. Allicht zijn er docenten die ook iets hiervan willen doorgeven aan hun leerlingen.
Dit artikel kent de volgende opbouw: na het kort vermelden van twee belangrijke resultaten uit de getaltheorie in paragraaf 2, beschrijven we kort, in de paragrafen 3, 4 en 5, de basis van RSA, hoe sleutelparen bij RSA er uitzien en hoe versleutelen en ontsleutelen werkt, en wat kraken van een sleutelpaar betekent. Daarna behandelen we twee methoden om een RSA-sleutelpaar te kraken: in paragraaf 6, nog in dit deel, de methode van Fermat die direct werkt op het ontbinden van bepaalde, verkeerd gekozen, grote getallen, en in het te verschijnen tweede deel van dit artikel, in paragraaf 7, de methode van Wiener die op een andere manier de privésleutel aanvalt als die zwak gekozen is. Beide methoden leiden tot een volledige kraak van het slecht gekozen RSA-sleutelpaar, en berusten op elementaire getaltheorie. We sluiten dan concluderend af in paragraaf 8.

2. Getaltheorie

RSA is gebaseerd op elementaire getaltheorie, en wel op modulo-rekenen met een vaste *modulus*. Zo'n modulus is een vast geheel getal n, en modulo-rekenen betekent dat bij het rekenen veelvouden van n 'verwaarloosd' worden, zoals we bij klokrekenen een veelvoud van 12 (of 24) niet meenemen. De notatie hiervoor is: $a \equiv b \pmod{n}$ als $a - b$ een veelvoud van n is. In zo'n geval 'identificeren' we a en b, net zoals we zeggen dat het 2 uur na 11 uur niet 13 uur is, maar 1 uur, want $11 + 2 = 13 \equiv 1 \pmod{12}$.
De rekenregels voor optellen, aftrekken en vermenigvuldigen gelden ook voor modulo-rekenen. Daarbij maakt het voor het antwoord niet uit op welk moment (vóór de berekening, of achteraf) er een veelvoud van de modulus bij een getal wordt opgeteld of afgetrokken. Meestal is het handig de getallen zo veel mogelijk terug te brengen naar de verzameling $\{0, 1, 2, \ldots, n-1\}$ door er het juiste aantal keer de modulus n van af te trekken of bij op te tellen.
Zo is bijvoorbeeld $25 \times (2 - 16) \pmod{17}$ te berekenen door eerst het gedeelte '(mod 17)' te negeren:
$25 \times (2 - 16) = 25 \times (-14) = -350$
en dan het juiste aantal malen 17 er bij op te tellen:
$-350 \equiv -350 + 21 \times 17 = 7 \pmod{17}$
Maar u mag net zo goed de 25 eerst vervangen door $25 - 17 = 8$ en de -16 door +1. Dan gaat het zo:
$25 \times (2 - 16) \equiv 8 \times (2 + 1) = 8 \times 3 = 24 \equiv 7 \pmod{17}$
Dat laatste heeft als voordeel dat de getallen altijd klein blijven.
Bij delen ligt het iets subtieler: dan geldt als extra voorwaarde voor het bestaan van de deling $a/b \pmod{n}$ dat de noemer b en de modulus n geen gemeenschappelijke deler hebben (anders dan 1). Daarop gaan we aan het eind van deze paragraaf nog kort in. Zie [2; de Weger] voor meer details.
Bij machtsverheffen is er iets aparts aan de hand. Omdat machtsverheffen niets anders is dan herhaald vermenigvuldigen, geldt dat als $a \equiv b \pmod{n}$ dan ook $a^2 \equiv b^2 \pmod{n}$, $a^3 \equiv b^3 \pmod{n}$, …, $a^k \equiv b^k \pmod{n}$, voor alle exponenten k.
Bijvoorbeeld, voor de machten van 7 modulo 15 vinden we:
$7^0 = 1$, $7^1 = 7$,
$7^2 = 49 \equiv 4 \pmod{15}$,
$7^3 = 7 \times 7^2 = 7 \times 4 = 28 \equiv 13 \pmod{15}$,
$7^4 = 7 \times 7^3 \equiv 7 \times 13 = 91 \equiv 1 \pmod{15}$.
En dan begint het van voren af aan:
$7^5 \equiv 7 \pmod{15}$, $7^6 \equiv 4 \pmod{15}$,
$7^7 \equiv 13 \pmod{15}$, enzovoorts.
Blijkbaar is $7^k \equiv 7^j \pmod{15}$ niet per se waar als $k \equiv j \pmod{15}$, maar wel als $k \equiv j \pmod{4}$.
De belangrijkste stelling in dit verband is de *Stelling van Euler*, die we hier alleen weergeven voor het speciale geval dat we bij RSA tegenkomen:



Invoer: twee positieve gehele getallen *a*, *b*
Uitvoer: $d = \text{ggd}(a, b)$, en *u*, *v* zodat $d = ua + vb$

$d_{nieuw} := a$; $d := b$; $u_{nieuw} := 1$; $u := 0$; $v_{nieuw} := 0$; $v := 1$

Herhaal
- Bereken het gehele deel *q* van d_{nieuw} / d, en de rest *r*
- Als de rest $r \neq 0$:
  - Dan: vervang d_{nieuw} door $(d_{nieuw} - qd)$; verwissel dan *d* en d_{nieuw}
    vervang u_{nieuw} door $(u_{nieuw} - qu)$; verwissel dan *u* en u_{nieuw}
    vervang v_{nieuw} door $(v_{nieuw} - qv)$; verwissel dan *v* en v_{nieuw}
    en ga door (met herhalen)
  - Anders: Stop (de herhaling)

Druk af: *d*, *u*, *v*

figuur 1 Uitgebreide algoritme van Euclides

Voorbeeld - Het berekenen van $d = \text{ggd}(62, 23)$

q	r	d_{nieuw}	$d\ (= r)$	u_{nieuw}	u	v_{nieuw}	v
		62	23	1	0	0	1
2	16	23	16	0	1	1	-2
1	7	16	7	1	-1	-2	3
2	2	7	2	-1	3	3	-8
3	1	2	1	3	-10	-8	27
2	0						

De conclusie is dat $\text{ggd}(62, 23) = 1 = -10 \times 62 + 27 \times 23$. Let erop dat in iedere regel van de tabel geldt dat $d = u \times 62 + v \times 23$.

Stelling van Euler **(*speciaal geval*):** Laten *p* en *q* twee verschillende priemgetallen zijn. Laat $n = pq$ (dit is de modulus) en $\phi(n) = (p - 1)(q - 1)$ (de ϕ-functie van Euler). Laat $a \in \{1, 2, \ldots, n - 1\}$ niet door *p* of *q* deelbaar zijn.
Dan geldt: $a^{\phi(n)} \equiv 1 \pmod{n}$.

Bij het rekenen modulo *n* geldt voor machtsverheffen, het berekenen van $a^k \pmod{n}$, dus dat de modulus *n* alleen voor het grondtal geldt, maar voor de exponent een andere modulus gehanteerd moet worden, namelijk $\phi(n)$.
Een algoritme dat we een paar keer nodig zullen hebben, is het *Uitgebreide Algoritme van Euclides*. Het algoritme van Euclides berekent de grootste gemene deler van twee getallen. De ggd van twee getallen is altijd een lineaire combinatie van die getallen, met andere woorden: als $d = \text{ggd}(a, b)$, dan zijn er gehele coëfficiënten *u* en *v* zodat $d = ua + vb$. Het uitgebreide algoritme van Euclides berekent met de ggd ook die coëfficiënten; ***zie figuur 1*** en het voorbeeld eronder.

De werking van het algoritme wordt verklaard door de volgende eigenschappen te zien:

- de verzameling van gemeenschappelijke delers van *d* en d_{nieuw} verandert bij het vervangen van d_{nieuw} niet; de grootste gemeenschappelijke deler dus ook niet; aan het begin van het uitvoeren van het algoritme is deze ggd(*a*,*b*), en aan het einde is *d* een deler van d_{nieuw} en is *d* dus ook de grootste gemeenschappelijke deler van *d* en d_{nieuw} en dus van *a* en *b*;
- bij het begin van het algoritme geldt $d = u \times a + v \times b$ (want dan is $u = 0$, $v = 1$ en $d = b$), de drie vervangregels in het algoritme behouden deze eigenschap, en ze geldt aan het eind dus nog steeds;
- zolang de rest niet 0 is, wordt d_{nieuw} vervangen door een getal dat echt kleiner is; het algoritme stopt dus na een eindig aantal stappen.

We geven nog een voorbeeld, met een toepassing op het delen bij modulo-rekenen (zie onder).

3. Sleutelparen bij RSA

RSA is een bekend cryptografisch systeem, genoemd naar Ron Rivest, Adi Shamir en Len Adleman, die het in de jaren '70 van de vorige eeuw bedacht hebben. RSA is onder andere geïmplementeerd in vrijwel alle webbrowsers, voor het beveiligen van internetcommunicatie.
RSA is een *asymmetrisch* of *publieke-sleutel-cryptosysteem*. Dat wil zeggen dat het werkt met *sleutelparen*. Een sleutelpaar is een tweetal bij elkaar behorende sleutels: een *publieke sleutel* en een *privésleutel*. Als RSA wordt gebruikt voor geheimschrifttoepassingen, dan moet met de publieke sleutel worden versleuteld, en met de privésleutel ontsleuteld.

Voorbeeld. Zoek *k* waarvoor geldt dat $46k \equiv 1 \pmod{77}$, mits *k* bestaat.
Dit kan door het uitgebreide algoritme van Euclides toe te passen op $a = 77$ en $b = 46$, want dat geeft $d = \text{ggd}(77, 46)$ en *u*, *v* met $d = 77u + 46v$.
Als het zo blijkt te zijn dat $d = 1$, dan zien we dat $46v = 1 - 77u \equiv 1 \pmod{77}$, en dan kunnen we dus $k = v$ nemen.
En als $d \neq 1$ blijkt te zijn, dan bestaat zo'n *k* niet, want dan zou *d* ook een deler van 1 moeten zijn.

d	r	d_{nieuw}	$d\ (= r)$	u_{nieuw}	u	v_{nieuw}	v
		77	46	1	0	0	1
1	31	46	31	0	1	1	-1
1	15	31	15	1	-1	-1	2
2	1	15	1	-2	3	3	-5
15	0						

De conclusie is dat zo'n *k* bestaat, en wel $k = -5$. Ter controle:
$46 \times (-5) = -230 \equiv -230 + 3 \times 77 = 1 \pmod{77}$
Merk op dat we hier in feite een deling hebben uitgerekend: $1/46 \pmod{77}$.

Een RSA-sleutelpaar wordt als volgt gemaakt. In paragraaf 4 zal dan duidelijk worden gemaakt dat met een op deze manier gekozen sleutelpaar handig kan worden versleuteld en ontsleuteld.

1. Kies een *veiligheidsparameter* s, het aantal bits dat nodig is om de modulus weer te geven in het tweetallig stelsel. Een op dit moment nog redelijk veilige keuze is $s = 1024$. Dat betekent dat we gaan werken met getallen in de orde van grootte van 2^{1024}; dat is ruim 300 decimale cijfers.
2. Kies twee willekeurige priemgetallen p, q van elk ongeveer ½s bits (met $s = 1024$ dus ruim 150 cijfers). Laten we $p > q$ nemen. We leggen hier niet uit waarom zulke grote priemgetallen bestaan, zelfs in grote overvloed, en hoe ze gevonden kunnen worden. Er zijn efficiënte methoden voor; zie [2; de Weger].
3. Bereken de *modulus* $n = pq$ van s bits (het zouden er $s - 1$ kunnen zijn, dat is niet erg; als u dat wel erg vindt, kies dan nieuwe p en q).
4. Bereken $\phi(n) = (p - 1)(q - 1)$.
5. Kies een *publieke exponent* e en een *privé-exponent* d, beide groter dan 2 en kleiner dan $\phi(n) - 2$, die de relatie $ed \equiv 1 \pmod{\phi(n)}$ bezitten. Dat kan als volgt. Kies één van de twee, willekeurig of volgens een bepaald stramien, zolang die exponent maar geen deler gemeen heeft met $\phi(n)$. Bereken dan de andere door het uitgebreide algoritme van Euclides toe te passen op de eerste gekozen exponent en $\phi(n)$. Zie het laatste voorbeeld onderaan pag. 257.
6. Gooi p, q en $\phi(n)$ weg, want die zijn niet meer nodig, en, ze mogen beslist niet in verkeerde handen vallen.
7. De publieke sleutel is nu het paar (n, e), en de privésleutel is het paar (n, d).

Voorbeeld met veiligheidsparameter s = 16.
$p = 211$, $q = 197$, $n = 211 \times 197 = 41567$
$\phi(n) = 210 \times 196 = 41160$
$e = 24377$, $d = 17393$
Nu is inderdaad aan de relatie $ed \equiv 1 \pmod{\phi(n)}$ voldaan, want:
$24377 \times 17393 = 1 + 10301 \times 41160$
De publieke sleutel is:
$(n, e) = (41567, 24377)$.
De privésleutel is: $(n, d) = (41567, 17393)$.

Opmerking. Bij het boek [2; de Weger] *hoort een webpagina met een Java-applet waarmee u dergelijke berekeningen zelf eenvoudig kunt uitvoeren, zelfs met grotere getallen. Het is aan te raden alle voorbeelden bij dit artikel na te rekenen, en ook eens met andere getallen te proberen. Een rekenhulpje als de genoemde applet is dan onmisbaar.*

De privésleutel (n, d) moet goed bewaakt worden door de eigenaar. Als de privé-exponent d in verkeerde handen valt, is de veiligheid van het sleutelpaar helemaal weg. De publieke sleutel (n, e) is daarentegen *echt* publiek: die mag aan iedereen bekend gemaakt worden. In het bijzonder moeten we ervan uitgaan dat ook een eventuele kraker de modulus n en de publieke exponent e weet.

4. Versleutelen en ontsleutelen met RSA

Veronderstel dat Benne een geheime boodschap aan Alda wil sturen, maar hij heeft alleen de beschikking over een onveilig communicatiekanaal (bijvoorbeeld het internet), dat namelijk wordt afgeluisterd door Karel. Alda heeft een RSA-sleutelpaar gemaakt, en heeft de publieke sleutel (n, e) aan Benne gegeven. De privésleutel (n, d) houdt zij angstvallig geheim. Benne codeert de boodschap tot een *bericht* in de vorm van een getal b, dat tussen 1 en n ligt, en geen deler met n gemeen heeft. Met behulp van Alda's publieke sleutel (n, e) kan hij nu het *geheimschrift* g berekenen als:
$g \equiv b^e \pmod{n}$
Dit geheimschrift stuurt hij naar Alda. Dat Karel het geheimschrift g kan afluisteren is helemaal niet erg; hij heeft immers niet de sleutel waarmee het ontcijferd kan worden. Alléén Alda heeft die privésleutel (n, d). Zij kan daarmee het bericht b weer terugvinden uit het geheimschrift g door het berekenen van:
$b \equiv g^d \pmod{n}$
Dit gaat goed, want de relatie tussen e en d geeft het bestaan van een k zodat:
$ed = 1 + k \cdot \phi(n)$
En nu volgt met behulp van de Stelling van Euler dat:
$g^d \equiv (b^e)^d = b^{ed} = b^{1+k \cdot \phi(n)} =$
$b \cdot (b^{\phi(n)})^k \equiv b \cdot 1^k = b \pmod{n}$

Voorbeeld
Stel dat Alda's sleutelpaar bestaat uit haar publieke sleutel: $(n, e) = (41567, 24377)$
en haar privésleutel: $(n, d) = (41567, 17393)$.
Benne wil het bericht 'lief' versturen aan Alda. Dat kan hij bijvoorbeeld coderen (volgens a=01, b=02, …, z=26) als de twee getallen: 1209, 506.
Benne versleutelt deze getallen met Alda's publieke sleutel als volgt:
120924377 ≡ 1671 (mod 41567)
50624377 ≡ 12949 (mod 41567)
Benne verstuurt als geheimschrift de getallen 1671, 12949 aan Alda. Een afluisteraar kan hier niets mee. Alleen Alda kan het geheimschrift ontcijferen met haar privésleutel, en wel als:
167117393 ≡ 1209 (mod 41567),
1294917393 ≡ 506 (mod 41567)
Uit de getallen 1209, 506 kan Alda meteen de boodschap 'lief' decoderen.

Terzijde. RSA wordt in de praktijk niet op de hierboven beschreven manier gebruikt. Daarvoor zijn de machtsverheffingen van grote getallen veel te veel rekenwerk. De boodschap wordt doorgaans met een veel efficiënter symmetrisch cryptosysteem, zoals AES (*Rijndael*)*, versleuteld. De sleutel daarvoor is klein* (128 *bits*)*, wordt door de verzender willekeurig gekozen* (*voor ieder bericht een andere*)*, en moet nu op een veilige manier naar de ontvanger gestuurd worden. Alleen de AES-sleutel wordt dan met RSA versleuteld; dat is wel efficiënt want het is maar een korte rij bits. De versleutelde sleutel wordt dan met het geheimschrift meegestuurd. De ontvanger moet nu eerst RSA gebruiken om de AES-sleutel terug te kunnen vinden, en kan dan daarmee het geheimschrift met AES ontsleutelen.*

5. Kraken van de RSA-sleutel

Een kraker heeft alleen de beschikking over publieke informatie, en wil daaruit graag geheime informatie achterhalen. Bij RSA bestaat de publieke informatie uit de modulus n en de publieke exponent e. Het doel van de kraker is de privé-exponent d te achterhalen, want dan kan hij geheime boodschappen gaan ontcijferen. De kraker kan wel raden dat de modulus twee priemfactoren heeft, maar niet welke dat zijn. Ook $\phi(n)$ kent hij niet.

Twee manieren om een RSA-sleutelpaar te kraken zijn:

- Proberen de modulus n te ontbinden in zijn factoren: $n = p \cdot q$. Als u dat kunt, dan kunt u makkelijk $\phi(n) = (p-1)(q-1)$ berekenen, en dan is het vinden van de privé-exponent d makkelijk, net zoals bij het maken van een sleutelpaar.
- Proberen direct de privé-exponent d te berekenen. Als u dat kunt, dan kunt u ook zonder p en q te weten ontsleutelen, want dat ging namelijk met $b \equiv g^d \pmod{n}$.

Van beide methoden geven we een voorbeeld, waarbij kraken lukt omdat het sleutelpaar op een zwakke manier gekozen was.

6. De methode van Fermat voor het ontbinden van de modulus

De eerste methode voor het kraken van RSA die we bekijken, grijpt alleen aan op de modulus, en probeert die te factoriseren. Het idee, afkomstig van de bekende Pierre de Fermat, is gebaseerd op het *merkwaardige product*

$X^2 - Y^2 = (X + Y)(X - Y)$

Hier zien we dat ieder verschil van twee kwadraten makkelijk te vinden factoren heeft. Voor oneven n is er altijd een triviale manier om n te schrijven als $X^2 - Y^2$, namelijk met

$X = ½(n + 1)$, $Y = ½(n - 1)$

Dit zegt niets over de priemfactoren van n, want nu is $X + Y = n$, $X - Y = 1$. U moet op zoek gaan naar andere X, Y met $n = X^2 - Y^2$ om een echte ontbinding te vinden. Omdat p en q priemgetallen zijn met $p > q$, zijn er geen andere oplossingen X, Y van $n = pq = X^2 - Y^2$ dan de bovengenoemde triviale, en de oplossing gegeven door $X + Y = p$, $X - Y = q$. En die oplossing is:

$X = ½(p + q)$, $Y = ½(p - q)$

Uit $p > q$ en $n = pq$ volgt dat $p > \sqrt{n}$. Een eenvoudige zoekmethode begint nu met X-en achtereenvolgens uit te proberen, te beginnen bij het kleinste gehele getal dat groter is dan $\sqrt{n}$ (het kleinste gehele getal groter dan of gelijk aan a geven we in hetgeen volgt aan met $\lceil a \rceil$). Bij iedere uit te proberen X gaan we na of $X^2 - n$ een kwadraat is. Zodra dat zo is stoppen we, en hebben we de oplossing gevonden. ***In figuur 2*** is een en ander als een algoritme weergegeven.

Het 'stopgetal' m is opgenomen om het algoritme niet langer te laten doorgaan dan gewenst. We laten in een voorbeeld zien hoe de methode werkt.

Invoer: te ontbinden n, en een 'stopgetal' m
Uitvoer: factoren van n, of een melding dat die niet gevonden zijn
$X := \lceil \sqrt{n} \rceil$; $i := 0$
Zolang $i < m$ Doe
    $Z := X^2 - n$
    Als Z een kwadraat is:
    Dan
        $Y := \sqrt{Z}$; $p := X + Y$; $q := X - Y$
        Druk af: p, q
        Stop
    Anders
        hoog X en i elk met 1 op, en ga door
Druk af: "Geen oplossing gevonden."

figuur 2 Ontbinden in factoren volgens Fermat

Voorbeeld

Neem $n = 41567$; dan is $\sqrt{n} = 203,87\ldots$; dus beginnen we met $X = 204$.
Dan is $Z = 204^2 - 41567 = 49$, en dat is meteen al een kwadraat, namelijk van $Y = 7$.
We vinden als ontbinding $41567 = (204 + 7)(204 - 7) = 211 \times 197$.
Neem nu $n = 41561$, dan is $\sqrt{n} = 203,86\ldots$, dus beginnen we weer met $X = 204$.
Dan is $Z = 204^2 - 41561 = 57$, en dat is geen kwadraat. Dus proberen we achtereenvolgens $X = 205, 206, \ldots$ totdat $Z = X^2 - 41561$ wel een kwadraat is.
Dat blijkt pas bij $X = 219$ te gebeuren: $Z = 219^2 - 41561 = 6400$, en dat is het kwadraat van $Y = 80$.
We vinden als ontbinding
$41561 = (219 + 80)(219 - 80) = 299 \times 139$.
(Merk op dat 299 geen priemgetal is; het is 13×23.)

De vraag is nu hoe goed dit algoritme van Fermat is. We willen achterhalen voor welke soorten sleutelparen de methode efficiënt werkt. We tellen daarom het aantal stappen, $i + 1$, dat het algoritme heeft doorlopen als het een oplossing p, q heeft gevonden. Bij die oplossing is $X = ½(p + q)$, $Y = ½(p - q)$, en $i = X - \lceil \sqrt{n} \rceil$, en natuurlijk ook $X^2 - Y^2 = n$. Nu is:

$$i = X - \lceil \sqrt{n} \rceil < X - \sqrt{n} = \frac{X^2 - n}{X + \sqrt{n}} = \frac{Y^2}{X + \sqrt{n}} < \frac{Y^2}{2\sqrt{n}} = \frac{(p-q)^2}{8\sqrt{n}}$$

Het aantal stappen is dus erg klein als de priemgetallen p en q dicht bij elkaar liggen. Om precies te zijn: bij een stopgetal m lukt het om n te ontbinden als:

$p - q < \sqrt{(8m)} \cdot n^{1/4}$

De priemgetallen p en q zijn ongeveer zo groot als $\sqrt{n}$, en hebben dus elk ongeveer half zoveel cijfers als n. Als nu hun verschil $p - q$ niet veel groter is dan $n^{1/4}$, dan hebben p en q dus bijna de bovenste helft van hun cijfers gemeenschappelijk. In zo'n geval kan het algoritme in een redelijk aantal stappen de ontbinding vinden. We geven een wat groter voorbeeld, van 64 bits.

Voorbeeld

$n = 16\,585\,512\,232\,168\,543\,399$; dan is $\lceil \sqrt{n} \rceil = 4\,072\,531\,429$;
$i = 0$: $X = 4\,072\,531\,429$;
$Z = X^2 - n = 8\,024\,238\,642$ is geen kwadraat;
$i = 1$: $X = 4\,072\,531\,430$;
$Z = X^2 - n = 16\,169\,301\,501$ is geen kwadraat;
$i = 2$: $X = 4\,072\,531\,431$;
$Z = X^2 - n = 24\,314\,364\,362$ is geen kwadraat;
$i = 3$: $X = 4\,072\,531\,432$;
$Z = X^2 - n = 32\,459\,427\,225 = 180\,165^2$ is een kwadraat. Dus:
$Y = 180\,165$, en
$p = X + Y = 4\,072\,711\,597$,
$q = X - Y = 4\,072\,351\,267$
Inderdaad komen de eerste 4 van de 10 cijfers (bijna de helft dus) van p en q overeen, en $(p - q)^2/(8\sqrt{n}) = 3,98\ldots$. Dat komt goed overeen met het feit dat we de ontbinding in 4 stappen hebben gevonden.

De conclusie van deze paragraaf is dat u bij het maken van een RSA-sleutelpaar niet de fout moet maken de twee priemgetallen te dicht bij elkaar te kiezen, maar op een afstand die flink groter is dan $n^{1/4}$. Anders levert dat een erg zwakke sleutel op.

Verwijzingen

[1] Ernst Lambeck e.a. (2008): *Geheim? Cryptografie en Getaltheorie*. Eindhoven: Regionaal Steunpunt Wiskunde D (zie *www.win.tue.nl/wiskunded*).

[2] Benne de Weger (2009): *Elementaire getaltheorie en asymmetrische cryptografie*. Utrecht: Epsilon Uitgaven (verschijnt voorjaar 2009).
Dit boek beoogt een toegankelijke tekst te zijn over (onder andere) RSA en de onderliggende getaltheorie. Bij het boek hoort een webpagina met een Java-applet, waarmee alle rekenbewerkingen waarvan in dit artikel sprake is, makkelijk uit-gevoerd kunnen worden, ook met grote getallen (zie *www.win.tue.nl/~bdeweger/MCR/*).

Over de auteur

Benne de Weger werkt als universitair docent cryptologie aan de Technische Universiteit Eindhoven.
E-mailadres: *b.m.m.d.weger@tue.nl*



Op weg naar 2014

STAND VAN ZAKEN ROND DE NIEUWE EXAMENPROGRAMMA'S HAVO/VWO

[Paul Drijvers]

Op 11 maart 2009 heeft de staatssecretaris van OCW, mevrouw Van Bijsterveldt, in een brief aan de Tweede Kamer ingestemd met de door cTWO opgestelde concept-examenprogramma's wiskunde A, B en D voor havo en vwo en C voor vwo. Deze examenprogramma's vormen de basis voor examenexperimenten, die in het schooljaar 2009-2010 van start gaan in vierde klassen van een beperkt aantal pilotscholen.
Daarmee gaat de voorbereiding van de vernieuwing van het wiskundeonderwijs per 2014 een nieuwe fase in. Reden om u in dit artikel nader te informeren over de voorgeschiedenis hiervan, de belangrijkste overwegingen van de vernieuwingscommissie, de meest in het oog springende veranderingen en de plannen van cTWO voor de nabije toekomst.

Voorgeschiedenis

Hoe zat het ook weer? Bij alle bètavakken lopen er veranderingsprocessen die leiden tot inhoudelijke herzieningen van de examenprogramma's havo en vwo. De andere vakken liggen daarbij voor op wiskunde. Dit voorjaar worden in het havo de eerste experimentele centrale examens scheikunde, natuurkunde en biologie afgenomen en worden wiskunde D en NLT middels schoolexamens afgerond.
Ook voor wiskunde heeft het ministerie van OCW een vernieuwingscommissie in het leven geroepen, die zichzelf *commissie Toekomst WiskundeOnderwijs* (cTWO) heeft gedoopt en onder voorzitterschap staat van Dirk Siersma, emeritus-hoogleraar wiskunde aan de Universiteit Utrecht.
De opdracht van cTWO omvat het opstellen van examenprogramma's voor wiskunde A, B, D voor havo en vwo en C voor vwo per 2014 en het adviseren over doorlopende leerlijnen en didactische ontwikkelingen.
cTWO is haar werk begonnen met het schrijven van een visiedocument dat de uitgangspunten voor het toekomstige wiskundeonderwijs beschrijft en daarmee richtingbepalend is voor de te ontwerpen examenprogramma's [cTWO, 2007; Siersma & Drijvers, 2007]. Een volgende stap was het ontwerpen van de examenprogramma's. De eerste versies daarvan zijn in het voorjaar van 2008 aan OCW aangeboden [Krüger, 2008abc]. Het ministerie was daarmee echter niet gelukkig, onder andere vanwege de reactie van de resonansgroep [Van de Craats, 2009]. Het ministeriële standpunt stuitte op haar beurt weer op verzet uit het veld [Kemme, 2008]. Na raadpleging van onder meer VSNU en HBO-raad heeft cTWO een revisie gepleegd, met de huidige concept-examenprogramma's als resultaat. In de aanpassingen heeft cTWO haar visie en ingezette koers in belangrijke mate kunnen combineren met de wensen van de staatssecretaris. In dit artikel gaan we vooral in op de laatste fase, die van de revisie van de examenprogramma's. De teksten van de programma's zijn te vinden op de website van cTWO (*www.ctwo.nl*).

Overwegingen en uitgangspunten bij de revisie

Welke uitgangspunten hebben bij de totstandkoming van de concept-examenprogramma's een rol gespeeld? We staan hieronder stil bij overwegingen rond basisvaardigheden, ICT-gebruik, denkactiviteiten, voorkennis uit onderbouw en overladenheid.

Basisvaardigheden

Het belang van goede basisvaardigheden wordt vanuit het hoger onderwijs benadrukt en ook door cTWO onderschreven. Dit heeft de concept-programma's dan ook in belangrijke mate beïnvloed. Het herstel van basisvaardigheden kan echter niet tot 2014 wachten. Sterker nog, er zijn duidelijke signalen dat dit herstel al in volle gang is. Om dit in kaart te brengen heeft het projectteam van cTWO een tussenevaluatie uitgevoerd van de 2007-programma's [cTWO, 2009]. Wiskundedocenten hebben een enquête ingevuld ($n = 193$), een beperkt aantal docenten is geïnterviewd, de 2007-edities van schoolmethodes zijn vergeleken met de voorgaande edities en leerlingen van klas 5 en van klas 6 hebben een vergelijkende algebratoets gemaakt (***zie figuur 1***). De resultaten van dit alles suggereren een duidelijke trend naar een betere beheersing van de algebraïsche vaardigheden. Zo presteren leerlingen van vwo-5, die het 2007-programma doorlopen, beter dan leerlingen van vwo-6 (oude programma). cTWO heeft de stellige verwachting dat het herstel van de algebraïsche vaardigheden, zoals ingezet in het 2007-programma, voldoende garantie geeft voor de aansluiting met het hoger onderwijs en acht verdere aanscherping op dit punt niet nodig.

ICT-gebruik

In 2008 heeft cTWO het rapport *Use to learn; naar een zinvolle integratie van ICT*

figuur 1

	Klas 5 (B-2007)	Klas 6 (B1 en B12)	Factor waarmee klas 5 beter scoort dan klas 6
breukvormen	60%	40%	1.5
wortelvormen	38%	30%	1.3
haakjes	62%	55%	1.1
machten	44%	34%	1.3
herleiden	66%	49%	1.3
vergelijkingen	63%	60%	1.1
log. vormen	25%	13%	1.9
exp. vergelijkingen	19%	25%	0.8
inzicht	20%	20%	1.0

De belangrijkste wiskundige functionaliteiten van ICT voor vwo wiskunde C zijn:

- FGT: Formules, grafieken en tabellen
  Denk aan de grafische rekenmachine, VU-Grafiek of Excel.
- DGM: Dynamische Grafieken en Meetkunde
  Denk aan Cabri, GeoGebra, TI-Nspire, Geocadabra of Doorzien.
- SGSS: Statistische Gegevensverwerking en Statistische Simulatie.
  Denk aan Excel, grafische rekenmachine, VU-Statistiek of SPSS.

In de volgende tabel staat in welke domeinen welke didactische en wiskundige ICT-functionaliteiten kunnen worden ingezet.

ICT-gebruik in vwo wiskunde C	Didactische functie ICT		
Domein	gereedschap	oefening	begripsvorming
B Algebra en tellen		FGT	
C Verbanden	FGT		FGT
D Verandering	FGT		
E Statistiek en kansrekening	SGSS		SGSS
F Logisch redeneren			
G Vorm en ruimte	DGM		DGM
H Keuzeonderwerpen			

figuur 2

Verdeling CE – SE		
Domein	CE	SE
A Vaardigheden	X	X
B Algebra en tellen	X	
C Verbanden	X	
D Verandering	X	
E Statistiek en kansrekening		X
F Keuzeonderwerpen		X

figuur 3

in het wiskundeonderwijs uitgebracht. Daarin worden wiskundige en didactische functionaliteiten van ICT-middelen voor het wiskundeonderwijs geïnventariseerd. Om deze inventarisatie te vertalen naar de praktijk, wordt in de toelichtingen van de gereviseerde concept-examenprogramma's aangegeven welke didactische en wiskundige functionaliteiten van ICT bij de verschillende domeinen van het betreffende vak van pas kunnen komen. ***Figuur 2*** geeft een voorbeeld hiervan voor wiskunde C van vwo. Daarnaast vermelden de subdomeinen A3 van de verschillende examenprogramma's ICT-vaardigheden als exameneis. Geadviseerd wordt het gebruik van de grafische rekenmachine op het centraal examen wel toe te staan maar aan dit gebruik op zichzelf geen punten toe te kennen. De toetsing van ICT-vaardigheden dient plaats te vinden in het schoolexamen. Voor de uitsplitsing SE – CE zijn overigens overzichten in de examenprogramma's opgenomen (***zie figuur 3***).

Denkactiviteiten

In het visiedocument van cTWO wordt veel aandacht besteed aan zogeheten denkactiviteiten. Als fundamentele denkactiviteiten voor wiskunde worden beschouwd modelleren en algebraïseren, ordenen en structureren, analytisch denken en probleemoplossen, formules manipuleren, abstraheren, en logisch redeneren en bewijzen. Dat is mooi, maar hoe zien we dit in de examenprogramma's terug? Om ervoor te zorgen dat de denkactiviteiten niet alleen zelf abstracties blijven, is in de revisie in de toelichtingen op de examenprogramma's aangegeven welke domeinen aanknopingspunten bieden voor welke denkactiviteiten. Tevens is verband gelegd tussen denkactiviteiten en de vaardigheden van domein A, die daarmee ook meer 'kleur' krijgen.

Figuur 4 geeft een voorbeeld van een dergelijk overzicht voor wiskunde B van havo. Vanzelfsprekend is dit niet meer dan een eerste aanzet tot het concretiseren van deze denkactiviteiten, die moet worden uitgewerkt in syllabi, lesmateriaal, en in onderwijs- en examenpraktijk.

Voorkennis uit onderbouw

De nieuwe programma's voor de Tweede Fase van havo en vwo veronderstellen vanzelfsprekend een bepaalde voorkennis. Om die te expliciteren heeft cTWO een trajectenboek wiskunde havo/vwo onderbouw gepubliceerd, waarin de vereiste vaardigheden worden beschreven. Het trajectenboek bevat een opsomming per leerjaar en per leerlijn van onderwerpen die aan bod kunnen komen, een en ander toegelicht met voorbeelden. Op basis hiervan is als onderdeel van de revisie een zogeheten voorkennisdocument ontwikkeld, dat het scharnier vormt tussen trajectenboek onderbouw en examenprogramma's en dat samenvat welke voorkennis men nodig heeft om in klas 4 met succes aan het programma te kunnen beginnen. Hiermee zijn de ingangseisen voor de Tweede Fase vastgesteld. Dit voorkennisdocument is ook bedoeld als bijlage bij de syllabi en de handreikingen van de examenprogramma's.

Figuur 5 toont een 'snapshot' uit het voorkennisdocument voor wiskunde B van vwo. Overigens zal cTWO de komende jaren meer aandacht aan de onderbouw van havo en vwo gaan besteden.

Overladenheid

Overladenheid is een belangrijk aandachtspunt bij onderwijsvernieuwing. cTWO gaat ervan uit dat de gereviseerde concept-programma's studeerbaar en onderwijsbaar zijn in de beschikbare studielast. Argumenten daarvoor zijn ontleend aan de ervaringen met de huidige 2007-programma's, aan de ervaringen van experimenteerscholen die op dit moment op kleine schaal met onderdelen uit de nieuwe programma's experimenteren, en op inschattingen van ervaren docenten. Daarnaast geven de bovengenoemde feiten rond het herstel van basisvaardigheden en de versterking van de onderbouw ook aanleiding op dit punt optimistisch te zijn. Dit neemt niet weg dat de inschatting van overladenheid een moeilijke zaak is. De syllabi zijn hiervoor mede bepalend, maar doorslaggevend zijn natuurlijk de ervaringen van de examenpilots. De monitoring van de experimenteerscholen zal hierop alert zijn. Mocht daarbij alsnog overladenheid worden geconstateerd, dan moeten bijstellingen worden gepleegd. Het tijdpad van invoering maakt dat zeker mogelijk.

Belangrijkste wijzigingen per vak

Na deze beschouwingen van meer algemene aard worden hieronder de belangrijkste wijzigingen beschreven in de gereviseerde concept-examenprogramma's ten opzichte van de huidige 2007-programma's, waarbij en passant ook nog wordt ingegaan op de revisie ten opzichte van de eerdere cTWO-versies van 11 januari 2008.

Wiskunde A

In het havo-programma wiskunde A is de belangrijkste wijziging dat de aanpak van Statistiek en kansrekenen is herzien. Uitgangspunt is hierbij de statistische analyse van grote datasets waarbinnen de wetmatigheden van de kansrekening een plaats kunnen krijgen [Van Streun & Van de Giessen, 2007ab]. Daarnaast wordt in het programma explicieter aandacht besteed aan rekenvaardigheden en algebraïsche vaardigheden.

Bij vwo wiskunde A zijn in de analyse (domeinen C, Verbanden, en D,

Subdomeinen havo wiskunde B	Mo - Al	Or - St	An - Pr	Fo	Ab	Lo - Be
B1: Standaardfuncties	X	X	X	X		
B2: Vergelijkingen en ongelijkheden	X	X	X	X		
B3: Evenredigheidsverbanden		X	X	X		X
B4: Periodieke functies	X	X	X			X
C1: Afstanden en hoeken in concrete situaties			X	X		
C2: Analytische methoden	X		X	X		
C3: Vectorrekening	X			X	X	
D1: Veranderingen	X	X		X		
D2: Afgeleide functies 1				X	X	
D3: Bepaling afgeleide functies		X		X		
D4: Toepassing afgeleide functies	X		X	X		

Mo - Al = Modelleren en algebraïseren (eindterm A2)
Or – St = Ordenen en structureren (eindterm A1)
An - Pr = Analytisch denken en probleemoplossen (eindterm A2 en A3)
Fo = Formules manipuleren (eindterm A3)
Ab = Abstraheren (eindterm A3)
Lo - Be = Logisch redeneren en bewijzen (eindterm A3)

figuur 4

Verandering) de e-macht en de ln-functie aan de standaardfuncties toegevoegd. Er is een apart subdomein Algebra. Grafen en matrices, lineair programmeren en discrete dynamische modellen maken geen deel uit van het verplichte programma, maar zijn wel kandidaat-keuzevakken.
Het domein E, Statistiek en kansrekenen, kent net als bij havo een andere opzet vanuit grote databestanden. Daarmee wordt een betere voorbereiding beoogd op het vervolg-onderwijs. De voorgenomen onderwerpen correlatie en regressie en betrouwbaarheids-intervallen, die wel in de 2008-versie van de cTWO programma's stonden, zijn geschrapt, maar kunnen wel in de keuzeruimte aan de orde komen. Er zal lesmateriaal voor worden ontwikkeld, dat in de pilotscholen wordt uitgetest.

Wiskunde B
In de B-programma's is een grotere nadruk komen te liggen op algebraïsche vaardigheden, onder meer als geïntegreerd onderdeel binnen de analytische meetkunde.
Bij havo wiskunde B is de ruimtemeet-kunde verplaatst naar wiskunde D. Analytische meetkunde en optimaliseren in de meetkunde zijn in het B-programma opgenomen.
Bij vwo wiskunde B is de nadruk op synthetische meetkunde en bewijzen vervangen door een accent op meetkunde met coördinaten, dat een combinatie omvat van algebraïsche en algemeen meetkundige technieken om meetkundige problemen aan te pakken. De discrete analyse is grotendeels vervallen.

Wiskunde C
Bij vwo wiskunde C is het domein Grafen en Matrices vervallen. Nieuw zijn domeinen Vorm en Ruimte en Logisch redeneren.
Het domein E, Statistiek en kansrekenen, kent net als bij wiskunde A een opzet vanuit grote datasets. Daarmee wordt een betere voorbereiding beoogd op het vervolg-onderwijs. De voorgenomen onderwerpen hypothesetoetsing, correlatie en regressie en betrouwbaarheidsintervallen zijn geschrapt, maar kunnen wel in de keuzeruimte aan de orde komen. Er zal lesmateriaal voor worden ontwikkeld, dat in de pilotscholen wordt uitgetest.
In vergelijking met de eerdere versie van cTWO is het domein Analyse van en reflectie op de rol van wiskunde vervangen door een globalere eindterm over de maatschappelijke, culturele en historische betekenis van wiskunde in subdomein A2, Profielspecifieke vaardigheden.

Wiskunde D
Bij havo wiskunde D is de formulering van de eindtermen in domein B, Statistiek en kansrekening, gewijzigd om het domein beter te onderscheiden van het gelijknamige domein in wiskunde A. Dit op basis van ervaringen van docenten met het huidige programma. Daarnaast heeft een herverkaveling van meetkundeonderwerpen tussen wiskunde B en D plaatsgevonden
Om Kansrekening en statistiek ook bij vwo wiskunde D beter te profileren ten opzichte van het overeenkomstige domein in wiskunde A en C, is het subdomein Ordenen, verwerken en samenvatten van statistische gegevens vervallen. In plaats daarvan is toegevoegd het subdomein Correlatie en regressie. Verder ook hier een herverkaveling van meetkundeonderwerpen tussen wiskunde B en D.
Dankzij de inzet van de opleidingen wiskunde van de universiteiten bestaan er voor vwo inmiddels mooie en inspirerende modulen voor de verplichte stof en voor de keuzestof voor vwo wiskunde D. Voor havo wiskunde D ligt dat veel moeilijker. Door de grote diversiteit van hbo-opleidingen, waarin wiskunde vaak een ondergeschikte rol speelt, blijkt het lastig te zijn voor hogescholen om dit op te pakken.

Plannen voor de nabije toekomst
Hoe nu verder? Nu de concept-examen-programma's klaar zijn, is er veel werk aan de winkel. Allereerst worden de programma's door CEVO en SLO uitgewerkt in syllabi en handreikingen. Met Cito wordt overlegd over het ontwerpen van centrale examens en voorbeelden daarvan. Verder moet er natuurlijk lesmateriaal zijn voor de

Rekenen in de meetkunde	– formules voor het berekenen van oppervlakte driehoek en rechthoek – formule voor inhoud balk – hellingshoek – goniometrische verhoudingen sin, cos en tan	– omtrek, oppervlakte en inhoud berekenen van figuren (ook niet rechthoekige) via (globaal) rekenen – effect van vergroten en verkleinen op lengte, oppervlakte en inhoud berekenen – grootte van hoeken en afstanden berekenen in 2D en 3D figuren
Redeneren met constructies	– eigenschappen en definities	– bewijzen van eigenschappen van figuren – de stelling van Thales gebruiken – berekeningen met de stelling van Pythagoras – redeneren met eigenschappen van hoeken in een cirkel

figuur 5

leerlingen die medio 2009 het examen-experiment ingaan. Onder aansturing van het projectteam van cTWO is een aantal auteursgroepen hiermee aan de slag. Tevens zorgt het projectteam voor de contacten met de pilotscholen en ondersteunt het hen bijvoorbeeld bij het opstellen van nieuwe PTA's.

Een curriculum is natuurlijk meer dan een verzameling eindtermen. Daarom zal cTWO zich de komende tijd onder andere bezighouden met het concretiseren van de denkactiviteiten uit het visiedocument. Ook dient het gebruik van contexten en de rol van toepassingen gestalte te krijgen, om de in het visiedocument bepleitte 'blik naar buiten' vorm te geven.

Daarnaast zal de aandacht ook uitgaan naar de onderbouw. Het door cTWO geschreven trajectenboek onderbouw zal verder worden uitgewerkt in samenhang met ontwikkelingen rond doorlopende (reken-)leerlijnen. Er zijn ideeën om materiaal te ontwikkelen voor klas 3 van havo en vwo, en om handvatten te ontwikkelen die de wiskundige denkactiviteiten ook in de eerste twee klassen beter tot hun recht te doen komen.

Al met al genoeg uitdagingen dus voor de komende tijd…

Meedenkers en meewerkers zijn welkom!

Recente producten van cTWO op een rij

- *Experimentele examenprogramma's 2014* – de concept-programma's waarmee de experimenten van start gaan
- *Concept-examenprogramma's 2014: toelichting van de vernieuwingscommissie cTWO* – toelichtende tekst op de experimentele programma's
- *Trajectenboek onderbouw* – inhoudsbeschrijving van de onderbouw havo-vwo
- *Voorkennisdocument* – uit het Trajectenboek onderbouw gedestilleerd overzicht van het ingangsniveau van de Tweede Fase havo-vwo
- *Tussenevaluatie van de 2007-programma's wiskunde havo/vwo* – het rapport van het projectteam cTWO over de 2007-programma's
- *Use to learn. Naar een zinvolle integratie van ICT in het wiskundeonderwijs* – uitwerking van de visie op het gebruik van ICT in de wiskundeles

Deze documenten zijn beschikbaar op *www.ctwo.nl* onder Publicaties.

Referenties

- cTWO (2007): *Rijk aan betekenis, visie op vernieuwd wiskundeonderwijs.* Utrecht: cTWO.
- cTWO (2008): *Use to learn. Naar een zinvolle integratie van ICT in het wiskunde-onderwijs.* Utrecht: cTWO.
- cTWO (2009): *Tussenevaluatie van de 2007-programma's wiskunde havo/vwo.* Utrecht: cTWO.
- J. van de Craats (2009): *Twee bewogen jaren.* In: *Euclides* 84(5); pp. 180-184.
- J. Krüger (2008a): *Wiskundeprogramma's veranderen.* In: *Euclides* 83(6); pp. 291-293.
- J. Krüger (2008b): *Wiskundeprogramma's veranderen: wiskunde A voor havo en vwo.* In: *Euclides* 83(7); pp. 332-335.
- J. Krüger (2008c): *Wiskundeprogramma's veranderen: wiskunde B voor havo en vwo.* In: *Euclides* 83(8); pp. 372-376.
- S. Kemme (2008): *Waarom het ministerie van OCW ongelijk heeft.* In: *Euclides* 84(1); pp. 26-29.
- D. Siersma, P. Drijvers (2007): *Rijk aan betekenis, het visiedocument van cTWO in vogelvlucht.* In: *Euclides* 82(5); pp. 169-172.
- A. van Streun, C. van de Giessen (2007a): *Een vernieuwd statistiekprogramma deel 1: Statistiek leren met data-analyse.* In: *Euclides* 82(5); pp. 176-179.
- A. van Streun, C. van de Giessen (2007b): *Een vernieuwd statistiek-programma deel 2: Data-analyse, een mogelijke opzet.* In: *Euclides* 82(6); pp. 217-221.

Over de auteur

Paul Drijvers is universitair hoofddocent bij het Freudenthal Instituut van de Universiteit Utrecht. Dit artikel schrijft hij als secretaris van de commissie Toekomst WiskundeOnderwijs.
De commissie is bereikbaar via e-mailadres *info@ctwo.nl* en URL *www.ctwo.nl*.

PI-dag in Nederland en Vlaanderen

14-03-09, OF, IN DE AMERIKAANSE SCHRIJFWIJZE, 3/14

Een comPIlatie van weblogs en persberichten betrekking hebbend op de PI-fotowedstrijd, samengesteld door de redactie van *Euclides*.

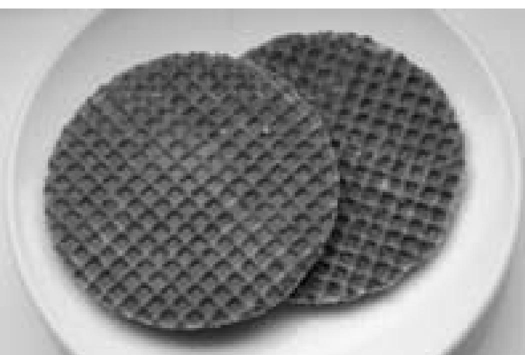
Vooraf

Herinnert u zich nog het artikel van Hans Wisbrun in *Euclides* 84(2) waarin hij ons meenam op zijn ontdekkingstocht naar de ChocoPi? Tijdens de studiedag op 8 november kon u een deze PI-chocoladeletter als vroeg Sinterklaasgeschenk kopen. Dit was nog maar het begin. Hans besloot een poging te wagen om de viering van PI-dag in Nederland en Vlaanderen flink te stimuleren. Op zijn weblog schrijft hij: 'Begin januari 2009 bedacht ik dat een prijsvraag een middel zou kunnen zijn om PI-dag in Nederland op de kaart te zetten. Al heel snel daarna vond ik de Wiskundemeisjes, Jeanine Daems en Ionica Smeets, en Vicky Vermeulen van Uitgeverij die Keure bereid aan deze poging publicitair mee te werken. Met Vicky kwam ook Vlaanderen in zicht. Mijn initiatief groeide flink uit toen redacteur Paul Steenhuis van het NRC-Handelsblad zich meldde en de prijsvraag op 14 februari in de krant werd aangekondigd. PI-dag staat hier nu echt op de kaart en zal dat blijven, daarvan ben ik overtuigd.'

Stroopwafels

Als we even terug gaan in de PI-geschiedenis, vinden we enthousiastelingen die al sinds jaar en dag PI-dag vieren op school. Op het weblog van Daaf Spijker lezen we dat hij al jaren klassikaal viert, met stroopwafels: 'Eerst uitdelen, aan elke leerling één. En dat "opgedrukte" vierkantjes-patroon (***zie foto 1***) is dan handig om een benadering van de oppervlakte van zo'n wafel te berekenen. De straal in het kwadraat is daarmee ook gemakkelijk te vinden. Dan delen, en na het rekenen: eten!
Het kan eventueel nog een keer, maar dan thuis (in de vakantie) op 22/7 (dat is *PI- benaderingsdag*).'

foto 1



Pi-kante soep

En uit een persbericht uit 2008 over de PI-ttige docenten en studenten van de Katholieke Hogeschool Mechelen citeren we: 'De leerlingen van het eerste en tweede jaar van het departement Lerarenopleiding van de Katholieke Hogeschool kwamen ook met een leuk initiatief op de proppen. Studenten en docenten konden er op 14 maart genieten van een groot eetfestijn in hun cafetaria onder het motto "Wiskunde, dat smaakt naar meer". Op het menu stond als voorgerecht een PI-kant tomatensoepje, gevolgde door een PI-taschotel met looksaus en frietjes als hoofdgerecht. Als dessert kon iedereen genieten van een PI-kdonkere chocolademousse. Om de dorst te lessen werd er door de studentenvereniging PI-sang Ambon aangeboden aan de aanwezigen. En raad eens hoeveel je voor het volledige menu moest betalen? Inderdaad, … 3,14 euro.'
En dezelfde hogeschool organiseerde al in 2007, ook toen al onder leiding van docente Conny van den Brande, een PI-evenement in samenwerking met een school voor speciaal onderwijs. De studenten wiskunde van de opleiding tot leraar organiseerden een PI-spel op de speelplaats (leerlingen gingen op zoek naar cijfers van het getal PI), ze maakten een PI-lied dat aan de leerlingen werd aangeleerd. Daarnaast kregen de leerlingen een djembé-introductie. De PI-medaille en PI-koekjes konden natuurlijk niet ontbreken!



foto 2

Eervolle vermeldingen

Dit jaar deden de wiskundestudenten uit Mechelen uiteraard mee met de fotowedstrijd. Ze kregen een eervolle vermelding met hun foto 'Drie keer π' (***zie foto 2***). In het juryrapport staat over deze foto: 'Een eervolle vermelding voor *de Katholieke Hogeschool Mechelen, departement lerarenopleiding, groep 1 BALSO wiskunde* (ook Vlaanderen). De foto is wat het object betreft (de drie π's) heel creatief, kunstzinnig, acrobatisch, enzovoort, maar de kwaliteit van de foto is niet zo goed.'
De andere eervolle vermelding was, ex aequo, voor *VTI Sint-Lucas* (Oudenaarden,



foto 3

nogmaals Vlaanderen). In het juryrapport lezen we (***zie foto 3***): ‘De tweede foto is weer een krachtige π, die vertedert (let op het vasthouden van de handjes), het groen oogt fris. Maar het is toch een mindere π dan die van de winnaar. Het oranje lijntje op de foto leidt ook af.’

De wedstrijd
Er kwamen 40 à 50 inzendingen binnen op de foto-oproep. De kwaliteit bleek boven verwachting en heel divers, zowel wat betreft uitvoering als afkomst. Wat die afkomst betreft: schoolklassen uit basis- en voortgezet onderwijs zijn ruim vertegenwoordigd. Maar ook individuen namen deel. En werknemers van een bedrijf, een fotocollectief, een dorpsacademie, een verkennersgroep, zelfs een groep scuba-duikkinderen (snorkelend en op drie meter diepte). De academische (wiskunde)wereld bleek zich te verschuilen achter lego-poppetjes.
Verderop in het juryrapport: ‘Dat, ook in de wiskundige betekenis van het woord, een groep niet per se uit personen hoeft te bestaan, realiseerde ik me al bij de allereerste inzending. Inzendingen met lieveheersbeestjes, plastic poppetjes, gymschoenen, smarties, enzovoorts vallen dan ook gewoon binnen de eisen van de opdracht. In de opdracht stond ook dat er ‘van bovenaf’ gefotografeerd moest worden. Waarom eigenlijk? Als de π maar duidelijk genoeg was! Als er anders gefotografeerd is, zoals bij een van de inzendingen die een eervolle vermelding gekregen heeft, hebben we die inzending daarom toch beoordeeld. Door de ervaring van nu wijzer geworden zal bij een herhaling in komende jaren misschien volstaan kunnen worden met een opdracht als ‘Doe een π-dansje en zet het filmpje op YouTube’. U bent er creatief genoeg voor!’

De jury, bestaande uit Hans Wisbrun, de Wiskundemeisjes en Lena *HireMyDNA* Shafir (kunstenares), koos uiteindelijk als winnaar de inzending van de *KSO Glorieux Ronse* (uit Ronse in Vlaanderen); ***zie foto 4***. Uit het juryrapport: ‘Niet alleen is de π heel duidelijk, de foto is ook mooi, qua compositie, scherpte en contrast, bijna een kunstwerk. Deze foto kwam dan ook op alle vier de lijstjes van de juryleden voor.’

Op naar 2010
PI-dag 2009 lijkt geslaagd te zijn en Hans Wisbrun kijkt al weer vooruit. Hij schrijft op zijn site: ‘Ik ben echter niet van plan een soort Nederlandse Mr Pi te worden. Het woord en de daad zijn in 2010 (volgend jaar valt PI-dag op een zondag) aan u. Organiseer creatieve evenementen, prijsvragen, sla desgewenst op de publicitaire trom.
Ik wil me wel vastleggen op het volgende. Bij leven en welzijn wil ik in 2010 weer zelf een grote prijsvraag organiseren: opdracht opstellen, jury samenstellen, sponsor regelen, ruchtbaarheid aan de prijsvraag geven, enzovoorts. De prijsvraagtekst zal voor het eerst in druk verschijnen in *Euclides* van februari 2010 na een *low-profile* introductie tijdens de Nationale Wiskundedagen 2010. Ook Vlaanderen zal rond die tijd bediend worden. (…) Tot PI-dag 2010!’

In Amerika wordt al jaren PI-dag gevierd. En volgens ons (de redactie van *Euclides*) is PI-dag de uitzondering op de regel dat je uit-Amerika-overgewaaide-‘feest’dagen, zoals Halloween en Valentijnsdag, beter kunt overslaan in je agenda.
14 maart 2010 staat bij ons in ieder geval genoteerd.

Internetadressen
Als u verder wilt lezen:
http://glorieuxronse.classy.be/pi.html
http://pi-dag.blogspot.com
www.wiskundemeisjes.nl
http://daafspijker.blogspot.com
www.shafir-etcetera.com/nl/home
www.teachpi.org/activities.htm
www.piday.org



foto 4 De winnaar!

Vanuit de oude doos

MCMXXX

[Ton Lecluse]

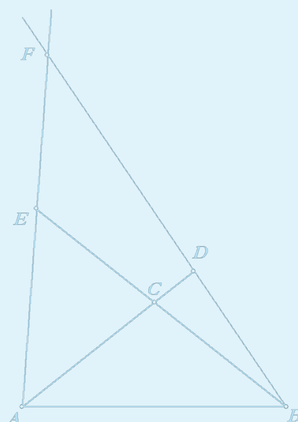
Ton Lecluse is docent wiskunde en heeft een doos met oude schoolboeken uit de vorige eeuw, waar hij graag in neust. Hij vindt vaak mooie opgaven (zonder uitwerking gelukkig) die hem uitdagen een oplossing te zoeken die past in het huidige curriculum. In de rubriek 'Vanuit de oude doos' wordt in elke aflevering een juweeltje behandeld. U kunt er uw lessen mee verrijken!

Een meetkundige plaats

Naar aanleiding van een toelatingsexamen wiskunde tot de universiteiten in 1930: Men verlengt de opstaande zijden CA en CB van een gelijkbenige driehoek met stukken AD en BE zodanig, dat $AD \times BE = AB^2$. Bewijs dat de meetkundige plaats van het snijpunt van de lijnen BD en AE een cirkel is.

U wordt eerst uitgedaagd een tekening te construeren die aan de gegevens voldoet. (Dan pas onder de streep spieken!) Wellicht helpt het dit model te tekenen met een dynamisch computerprogramma.

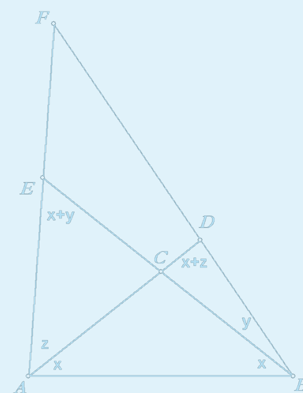
Het gegeven $AD \times BE = AB^2$ schrijven we eerst om tot $AD : AB = AB : BE$, waaruit volgt dat de driehoeken ADB en BAE gelijkvormig zijn (let op de *volgorde van de letters*). Het gelijkvormigheidscriterium *zhz* is hier van toepassing, mede omdat in deze driehoeken de hoeken A en B gelijk zijn. Driehoek ABC is immers gelijkbenig.



figuur 1

Het construeren van een figuur die hieraan voldoet, met een dynamisch meetkundeprogramma, is niet triviaal. Nadat u de gelijkbenige driehoek ABC heeft getekend en de opstaande zijden verlengd, kunt u (bijvoorbeeld) punt E vrij kiezen op de lijn door B en C.
Daarna kunt u hoek AEB overbrengen naar B, waardoor u de lijn door B heeft waarop het punt D moet liggen. Snijden met AC geeft D, enzovoort.
Wanneer u dan E sleept, lijkt het er inderdaad op dat het snijpunt F van AD en BE een cirkeldeel doorloopt.
Hoe nu verder? Niet verder lezen, eerst zelf proberen.

Uit de gegeven *gelijkbenigheid* en *gelijkvormigheid* kunt u conclusies trekken over hoeken die aan elkaar gelijk zijn (***zie figuur 2***).



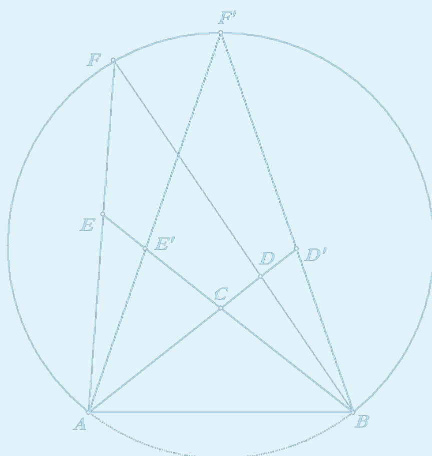
figuur 2

En nu? Niet verder lezen, eerst zelf proberen.

In driehoek ABD geldt:
$\angle A = x = 180° - \angle B - \angle D = 180° - (x+y) - (x+z)$.
In driehoek ABF geldt:
$\angle F = 180° - \angle A - \angle B = 180° - (x+z) - (x+y)$.
Dus $\angle F = x$, een hoek die niet verandert wanneer E wordt versleept over BC.
De stelling 'hoeken op dezelfde cirkelboog' zegt nu dat F een cirkelboog doorloopt met A en B als eindpunten.

Maar hoe moet je deze cirkelboog nu tekenen? Waar ligt het middelpunt?
Niet verder lezen, eerst zelf proberen.

Wanneer één punt F is geconstrueerd, kan de omgeschreven cirkel van driehoek ABF getekend worden, waarna de grote boog AB de oplossing is (met of zonder eindpunten?).



figuur 3

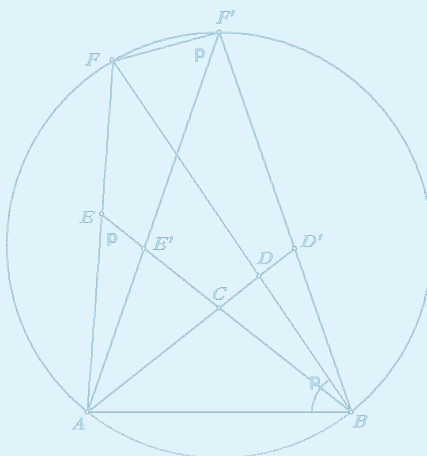
In figuur 3 is het punt F' zo gekozen dat driehoek ABF' gelijkbenig is: $AB = AD' = BE'$ (dan is driehoek ABD' congruent met driehoek ABE').

Tot slot

In figuur 3 is de meetkundige plaats van het punt F getekend wanneer punt E de halve lijn BC en (daarmee) punt D de halve lijn AC doorloopt.
In de opgave wordt gesproken over het *verlengde van CA* en *CB*. Wanneer u zich hieraan zou houden, is de oplossing de (kleine) cirkelboog tussen de snijpunten van CA en CB met de cirkel.

Wanneer E de *gehele* lijn door B en C doorloopt, is de meetkundige plaats van F dan de hele cirkel?
Tijdens het analyseren van de tekening ontdekte ik nog een mooie eigenschap van het model: de vierhoeken $EFF'E'$ en $DFF'D'$ zijn koordenvierhoeken.
Ziet u waarom? Niet verder lezen, eerst zelf proberen.

Zoals we al eerder zagen, zijn de driehoeken ADB en BAE gelijkvormig.



figuur 4

Dus: $\angle ABD = \angle BEA = p$. Dan is:
$\angle FEE' \,(= \angle FEB) = 180° - p$ (*gestrekte hoek*).
Ook geldt: $\angle ABD \,(= \angle ABF) = \angle AF'F = p$; het zijn omtrekshoeken op dezelfde boog AF.
Dus:
$\angle FEE' + \angle FF'E' = (180° - p) + p = 180°$. En dan is $EFF'E'$ een koordenvierhoek.
Een analoog verhaal kan gehouden worden voor vierhoek $DFF'D'$.

Bron

Dr. Th.G.D. Stoelinga, Dr. M.G. van Tol (1958): *Wiskunde-Opgaven van de toelatingsexamens tot de Universiteiten van 1925 tot en met 1958*. Zwolle: N.V. Uitgeversmaatschappij W.E.J. Tjeenk Willink (8e druk).

Over de auteur

Ton Lecluse is docent wiskunde aan het Comenius College te Hilversum.
E-mailadres: *alecluse@casema.nl*

Boekbespreking / Lewis Carroll in Numberland

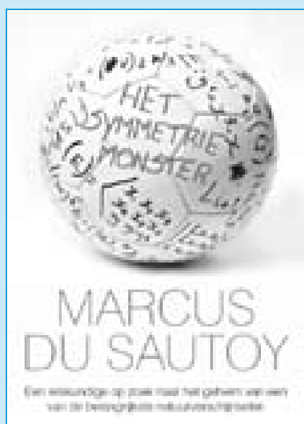


Ondertitel: His Fantastical Mathematical Logical Life
Auteur: Robin Wilson
Uitgever: Allen Lane (Penguin Group), Londen (2008)
ISBN: 978-0-71399-757-6
Prijs: ong. € 22,95 (gebonden, 237 pagina's)

Het boek begint met een aantal stukjes uit Carrolls fictie-boeken waarin wiskunde voorkomt. Daarna leest het als een biografie, met nadruk op de wiskundige ontwikkeling van Dodgson. Het is leuk om te zien welke vakken Dodgson deed en wat er in het negentiende-eeuwse Oxford gevraagd werd op tentamens. Ook legt Wilson een aantal wiskundige bijdragen van Dodgson uit, bijvoorbeeld zijn werk aan determinanten en zijn pogingen om een eerlijk verkiezingssysteem op te stellen. We lezen natuurlijk ook van alles over zijn familie, studiegenoten en docenten, en we lezen dagboekpassages waaruit blijkt dat voor Dodgson wiskunde soms ook gewoon moeilijk was.
De laatste paar hoofdstukken beschrijven de wiskundige raadsels waar Dodgson erg dol op was. Deze hoofdstukken zijn in feite een soort bloemlezing van de boeken met wiskundige puzzels en spelletjes die Dodgson onder zijn pseudoniem schreef voor een breed publiek, en van de puzzels die hij opgaf aan de kinderen met wie hij bevriend was. Wilson voegt hier nauwelijks iets toe, behalve af en toe wat uitleg, en persoonlijk had ik na een tijdje wel genoeg van Carrolls puzzels en raadsels: het is wat veel van hetzelfde. Daarna stopt het boek nogal abrupt, waar ik liever nog een nawoord of conclusie van Wilson gezien had, want nu ontbreekt de grote lijn een beetje.
Wat voor wiskundige was Dodgson eigenlijk? De indruk die bij mij bleef hangen na het lezen van het boek, is dat Dodgson iemand was met een creatieve geest die eindeloos gefascineerd werd door wiskundige rariteiten en puzzels, maar geen echt grote dingen aan de wiskunde heeft bijgedragen. En dat is ook niet zo raar: waarschijnlijk is Dodgson niet voor niets veel bekender als schrijver en fotograaf. Het boek leest lekker weg (behalve als er teveel puzzels na elkaar komen), Wilson citeert volop grapjes en absurditeiten uit de brieven en boeken van Dodgson en er staan veel leuke plaatjes en afdrukken van oude documenten in. De biografische delen vind ik goed, die heb ik met plezier gelezen. Er is weinig wiskundige voorkennis nodig, het boek is geschikt voor een breed publiek. Maar als je al redelijk bekend bent met Carrolls werk, staat in sommige hoofdstukken wel erg veel bekends, en daar voegt Wilson naar mijn smaak te weinig zelf aan toe.

Bron
www.wiskundemeisjes.nl / Jeanine Daems /

Verschenen / Het Symmetrie-monster



Auteur: Marcus du Sautoy
Oorspronkelijke titel: Finding Moonshine – A Mathematician's Journey through Symmetry
Vertaling: Fred Hendriks
Redactionele adviezen: Ionica Smeets
Uitgever: Uitgeverij Nieuwezijds, Amsterdam (2009)
ISBN: 978-90-5712-286-6
Prijs: € 24,95 (paperback, 360 pagina's)

Van de achterkant – Hoe is het om door een briljante ingeving een eeuwenoud wiskundig vraagstuk op te lossen? En om, tien minuten later, erachter te komen dat je daarbij een denkfout hebt gemaakt?
Marcus du Sautoy begint zijn persoonlijke zoektocht naar de geheimen van symmetrie op zijn veertigste verjaardag. Hij neemt de lezer mee op zijn reis van twaalf maanden rond de wereld en door de geschiedenis: van het Alhambra in Granada naar de Franse revolutie en van de *Goldberg Variaties* van Bach naar de piramiden van Gizeh. Een bont gezelschap van excentrieke wiskundigen uit alle tijden en windstreken komt in zijn verhalen tot leven.
Hoogtepunt is de meest spannende ontdekking in de wiskunde tot nu toe: het Monster, een gigantische sneeuwvlok die zich voordoet in een 196.883-dimensionale ruimte, met meer symmetrieën dan atomen in de zon. Met het wiskundig bewijs van deze sneeuwvlok werd het geheim van de symmetrie ontraadseld.

Marcus du Sautoy werd na zijn veertigste hoogleraar in The Public Understanding of Science van Oxford University (en als zodanig opvolger van Richard Dawkins) en is onder andere bekend als presentator van de BBC-serie *The Story of Maths*. Hij is tevens hoogleraar wiskunde in Oxford.

Verschenen / Wiskunde D

Uitgeverij Epsilon Uitgaven werkt aan materiaal voor het schoolvak **wiskunde D**. De teksten, die direct bruikbaar zijn in de les, zijn gratis te downloaden.
Op dit moment zijn vier delen beschikbaar.

Deel 1 – *F. Verhulst*: Dynamische Modellen versie 2.0
De tekst is geschikt voor leerlingen in vwo-5 en vwo-6. Het is een bijzonder toegankelijke tekst met veel voorbeelden, niet alleen de voor de hand liggende uit de biologie, maar ook uit de economie en natuurkunde.
Natuurlijk zijn er voldoende opgaven. U vindt hier de tweede versie van deze tekst. Deze is uitgebreid en verbeterd ten opzichte van de vorige versie.

Deel 2 – *A. van den Brandhof*: Kansrekening
Dat kansrekening veel meer is dan vazen en knikkers, wordt duidelijk in deze wiskunde D-tekst. Kansrekening is een serieuze tak van de wiskunde, die tal van raakvlakken heeft met andere onderwerpen uit de wiskunde, zoals analyse en meetkunde. Deze module is dan ook speciaal geschreven voor leerlingen met wiskunde B: er is kennis van de differentiaal- en integraalrekening nodig. In de appendices worden de belangrijkste zaken uit de combinatoriek, analyse, verzamelingenleer en meetkunde, die nodig zijn voor deze module, kort besproken.

Deel 3 – *H. Tijms*: Optimalisatie in Netwerken
Deze module is een avontuurlijke reis langs niet-aangeharkte paden door het gebied van de optimalisering in netwerken en richt zich op leerlingen in 5- en 6-vwo. De module bevat uitdagende stof voor zowel leerling als leraar en laat zien welke boeiende toepassingen de wiskunde in de praktijk heeft. Vele praktische problemen in uiteenlopende gebieden kunnen worden geformuleerd als een optimaliseringsprobleem op een netwerk: kortste-pad probleem, handelsreizigersprobleem, routeringsproblemen, etc.

Deel 4 – *G. Cornelissen*: Diophantische Vergelijkingen, mogelijkheden en onmogelijkheden
In het eerste gedeelte ('Mogelijkheden') worden een aantal diophantische problemen op een algebraïsche en meetkundige manier aangepakt. In het tweede gedeelte ('Onmogelijkheden') wordt besproken in hoeverre een computer in staat is om diophantische problemen op te lossen.
Zie ook: Steven Wepster (2009): *Diophantische vergelijkingen*. In: *Euclides* 84(6), pp. 212-213.

Website:
www.epsilon-uitgaven.nl/wiskunded.php

Aankondiging / Vakantiecursus 2009: tel uit je winst

De vakantiecursussen wiskunde zijn informatieve en inspirerende bijeenkomsten voor wiskundedocenten, al sinds 1946. Tijdens de cursus komen interessante onderwerpen ter sprake, met actuele toepassingen die de relevantie van wiskunde laten zien. Sprekers geven een beeld van de diversiteit van de beroepspraktijk. Het thema dit jaar is: **Tel uit je winst – wiskunde in geld en spelen**

Locatie 21 en 22 augustus: CWI, Amsterdam
Locatie 28 en 29 augustus: TU/e, Eindhoven

De vakantiecursus wordt georganiseerd door het CWI, in samenwerking met de Nederlandse Vereniging van Wiskundeleraren en wordt gesponsord door de Nederlandse Organisatie voor Wetenschappelijk Onderzoek.

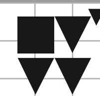


Het programma bestaat uit twee dagen (vrijdag van 15:00u tot 20:30u en zaterdag van 10:00u tot 15:00u) en wordt eerst bij het CWI (op 21 en 22 augustus) gegeven, en herhaald bij de Technische Universiteit Eindhoven (op 28 en 29 augustus).
Het exacte programma wordt bekend gemaakt op een later tijdstip.
Zoals alle jaren is de cursus voor alle wiskundedocenten – ook die bij het hbo – en belangstellenden interessant. Voor geïnteresseerden is een nascholings-certificaat beschikbaar.

Aanvragen brochure en aanmelding
Het CWI verzendt elk jaar een brochure over deze cursus. Wie deze brochure nog niet automatisch ontvangt, kan deze aanvragen via:
www.cwi.nl/Aanvraag_brochure_vakantiecursus_2009
Aanmelden kan met het aanmeldformulier achterin de brochure (in mei beschikbaar).
Het formulier moet vóór 10 augustus 2009 opgestuurd worden naar het CWI.
Aanmelden kan ook on line via:
www.cwi.nl/Aanmelding_vakantiecursus_2009

Cursusgeld en betaling
Het cursusgeld bedraagt € 75,00. Voor studenten aan lerarenopleidingen is het cursusgeld € 25,00.
Wijze van betaling: zo spoedig mogelijk na de inschrijving dient men het cursusgeld over te boeken naar bankrekening 31.35.57.977 (Rabobank) van de Stichting Wiskunde en Informatica Conferenties te Amsterdam, onder vermelding van uw naam en VC2009.
Betaling vanuit het buitenland: voor diegenen die vanuit het buitenland het cursusgeld willen overmaken, geldt de volgende extra informatie:
BIC: RABONL2U en IBAN: NL76RABO0313557977

Bron
www.cwi.nl/nl/events/2009/VC2009



Van de bestuurstafel

[Kees Lagerwaard, secretaris NVvW]

Zo ongeveer elke maand is er een bestuursvergadering. Tussendoor komt het Dagelijks Bestuur (voorzitter, penningmeester en secretaris) bij elkaar om lopende zaken door te nemen. Nogal wat thema's zijn vrij technisch van aard en betreffen organisatie en financiën. Andere thema's zijn meer inhoudelijk van aard. Daarover gaat deze bijdrage.

Eindexamens

Op het moment van verschijnen van dit nummer zitten we nog midden in de eindexamens. De eindexamens zijn afgenomen en waarschijnlijk ook al gecorrigeerd. Binnenkort vindt de normering plaats en weten we of er nog leerlingen aan de herkansing gaan deelnemen. We hebben dan de eerste havo-examens wiskunde A en B volgens het herziene examenprogramma achter de rug. We zijn benieuwd wat u van deze examens vindt. Vindt u de verwachte veranderingen door de PEP-operatie ook terug in de examens? Bent u ingenomen met dat herziene programma? Is het prettiger lesgeven? Zullen leerlingen beter zijn voorbereid op hun vervolgstudie? Aarzel niet uw mening daarover te geven op het forum op de site van de Vereniging. Examenprogramma's worden nogal eens gewijzigd en als je het als docent een keer hebt doorlopen, kun je er pas echt een goed oordeel over geven. Wij willen er graag zoveel mogelijk over horen.
Volgend jaar komen de eerste vwo-examens wiskunde A, B en C. En inmiddels zijn de syllabuscommissies alweer begonnen de nieuwe examenprogramma's, die door cTWO zijn geformuleerd, nader uit te werken. Deze programma's zullen over een aantal jaren de herziene 2007-programma's gaan vervangen. In de syllabuscommissies heeft ook een lid van het bestuur zitting. Het is de bedoeling dat er komend schooljaar al pilotscholen zullen gaan proefdraaien met die nieuwe programma's.
Inmiddels ziet het er naar uit dat we echt te maken gaan krijgen met een strengere zak/slaag-regeling. Onze voorzitter Marian Kollenveld heeft in de afgelopen tijd geprobeerd de politiek te wijzen op ongewenste effecten van deze regeling. Wanneer wiskunde zo'n cruciale rol krijgt bij het wel of niet slagen, is het gevaar groot dat leerlingen 'voorzichtiger' gaan kiezen. In geval van twijfel maar liever wiskunde A dan de misschien te moeilijke wiskunde B. Of liever in plaats van een profiel met wiskunde in havo het C&M-profiel zonder wiskunde. Dat kan toch niet de bedoeling zijn van de beleidsmakers? Marian is van plan nog een poging te wagen politiek Den Haag hiervoor te waarschuwen. Het Bestuur hoopt dat ze gehoord wordt.

RekenVOort

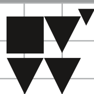
De Vereniging voert dit project uit in samenwerking met het Freudenthal Instituut. Er hebben zich een aantal leden aangemeld om mee te schrijven aan een lessencyclus rekenen voor leerlingen in vmbo en havo die geen wiskunde als examenvak hebben gekozen. Die schrijfactiviteit is inmiddels in volle gang. Ook zijn er voldoende scholen bereid gevonden om komend jaar deze modules rekenen te gaan uitproberen. Eind 2010 moet er dan een tweetal modules beschikbaar zijn. Er wordt zowel aan digitaal als aan papieren materiaal gewerkt.
Dergelijke activiteiten zijn nieuw voor ons. We hebben gelukkig voldoende enthousiaste en deskundige leden die een dergelijk project kunnen uitvoeren. En we hebben Gert de Kleuver als enthousiaste projectleider weten te strikken. Ook heeft het Freudenthal Instituut een belangrijke organisatorische en inhoudelijke inbreng. De Vereniging heeft echter geen bureau dat de financiële en administratieve werkzaamheden die ook aan zo'n project vastzitten, uitvoert. Dat zorgt voor extra werk voor sommige bestuursleden, en dat kan een zware last worden wanneer er meer projecten op het pad van de Vereniging komen. Er zijn op dit moment allerlei activiteiten gaande op het gebied van rekenen/wiskunde in het voortgezet onderwijs. Dat aantal is zo groot dat het gemakkelijk onoverzichtelijk en inefficiënt kan worden. Misschien ligt er voor de Vereniging ook wel een taak in het inventariseren en coördineren van al deze projecten. Dat zou kunnen leiden tot een optimale inzet van middelen en inzet om tot beter reken- en wiskundeonderwijs te komen.

Vmbo

Ook dit jaar is er maar één examenbespreking voor de vmbo-examens. En dat terwijl aan de BB, KB en GL/TL-examens door veel meer leerlingen wordt deelgenomen dan aan de wiskunde-examens op havo en vwo. Op BB-niveau doen vrijwel alle leerlingen het wiskunde-eindexamen op de computer. En volgend jaar zal er ook op KB-niveau, naast een papieren examen, een digitaal examen beschikbaar zijn. Er is dus op het vmbo veel in beweging. Was er voorheen bij KB en GL/TL een afwisseling van Statistiek en Meetkunde als een van de onderwerpen op het centraal examen, sinds een paar jaar zit Meetkunde elk jaar in het centraal eindexamen. Voor kandidaten uit de sector Techniek is dat misschien niet zo lastig, maar hoe ervaren de leerlingen uit de andere sectoren dit? Is het voor docenten lastig om deze leerlingen meetkunde te leren? Is statistiek gemakkelijker? We zouden zo graag met vmbo-docenten in contact komen om, bijvoorbeeld in de werkgroep vmbo, over allerlei aspecten van het vak te praten, ervaringen uit te wisselen en misschien initiatieven te ontwikkelen om het wiskundeonderwijs op het vmbo te kunnen verbeteren.

Werkgroep havo/vwo

Een afvaardiging van deze werkgroep was onlangs te gast op een bestuursvergadering. Onderwerp van gesprek was de door hen



ontwikkelde ‘exittoets’ bij wiskunde A vwo. In feite is deze toets ontwikkeld als reactie op de diverse entreetoetsen die op universiteiten worden ingezet om de algebraïsche vaardigheid van de instromende studenten in kaart te brengen en, vooral, om deficiënties vast te stellen. Vaak wordt er daarna een onderwijsmodule aangeboden om die deficiënties weg te werken. De werkgroep had nogal wat kritiek op een aantal van die toetsen. Soms bevatten ze vragen die de nieuwbakken studenten onmogelijk kunnen beantwoorden omdat ze niet tot de vwo-stof behoren. Ook was er nogal wat kritiek op de vraagformuleringen. Het verbod op het gebruiken van een (grafische) rekenmachine maakt het er ook al niet gemakkelijker op.
De werkgroep ontwierp een toets die past bij het wiskunde A-programma van het vwo, en die ook qua formuleringen herkenbaar is. Maar ook dit is een toets die alleen betrekking heeft op algebraïsche vaardigheden en daarmee dus op slechts een beperkt deel van de wiskunde A-stof. Daarom zou de term *exittoets* ten onrechte de indruk kunnen wekken dat het een afsluitende toets is die een vergelijkbare functie heeft als het eindexamen wiskunde A. De werkgroep beoogt met de toets echter een instrument aan te bieden dat een diagnostische functie heeft op het terrein van algebraïsche vaardigheden.
Vanuit het bestuur werd waardering uitgesproken voor het werk dat de werkgroep hiermee heeft geleverd. De toets zal inclusief een uitgebreide toelichting en een correctiemodel aan docenten beschikbaar worden. Bij een proefafname op een beperkt aantal scholen bleken de resultaten nogal tegen te vallen. Hopelijk wordt dat spoedig beter nu er in het aangepaste A-programma een prominentere plaats is ingeruimd voor algebra. Waarbij wel steeds met nadruk moet worden gesteld dat het een toets is op algebraïsche vaardigheden en *niet* op het vak wiskunde A. Voor dat laatste zijn schoolexamens en het centrale examen de aangewezen meetinstrumenten.
De werkgroep zal de toets ook presenteren middels een artikel in *Euclides*.

Wiskunde in het vmbo

[Henk Bijleveld]

Het nieuwe wiskundeonderwijs

Wat is de optimale didactiek van de wiskunde in het vmbo? De afgelopen jaren is wiskundeonderwijs in beweging en de 50 minuten durende monoloog van de docent waarbij de leerlingen passief in de banken zitten, is al lang verdwenen. Voor veel scholen is het een uitdaging om het wiskundeonderwijs een andere vorm te geven waarbij de leerlingen actief bezig zijn. Mijn vraag is: ‘Zijn alle veranderingen wel verbeteringen?’
Veel scholen werken met weekplanners, zoals die ook op basisscholen veel worden gebruikt. Leerlingen hebben de vrijheid om per week zelf een planning te maken en zelf te bepalen wanneer zij hun taken doen. Bij de ene school heet dit ‘activerende didactiek’, een andere school noemt het ‘bolwerken’, weer een andere noemt het ‘project’. Hierbij hoort ook dat de leerlingen hun eigen werk nakijken en beoordelen. Ze krijgen de vrijheid om aan het ene vak, waarmee ze moeite hebben, meer tijd te besteden dan aan een vak waarmee ze snel klaar zijn. Voorbeelden van scholen die met een dergelijk systeem werken, zijn Slash 21 en UniC.

De voordelen op een rijtje

Die nieuwe onderwijsvorm heeft zeker voordelen. De zelfstandigheid van de leerling wordt gestimuleerd. De prestatie van de leerling wordt duidelijk zichtbaar voor de begeleidende docent en de leerling kan dus niet opgaan in de massa. De leerling leert plannen en z’n tijd in te delen. Als hij zijn werk niet op tijd af heeft, is dat direct zichtbaar en kan er adequaat op worden ingespeeld.
De leerling wordt uitgedaagd om samen te werken. In de traditionele manier van les geven is samenwerking veel minder aan de orde. Als je als docent merkt dat een of meer leerlingen bepaalde onderdelen van de stof niet begrepen hebben, dan kun je ze even apart nemen en nog eens extra aandacht geven zonder dat de klas er op hoeft te wachten. Voor een moeilijk vak kunnen de leerlingen meer tijd nemen dan voor een vak dat ze makkelijker af gaat. Ze werken aan vaardigheden die ze later in het mbo en bij een arbeidsplaats nodig hebben.

En de nadelen …

Het gevaar bestaat dat er niet altijd, wanneer de leerling aan wiskunde wil werken, een wiskundedocent aanwezig is. Het is de bedoeling dat twee of drie klassen in een ruimte zitten, en dat er daarbij twee of drie docenten aanwezig zijn. Er zijn scholen waar leerlingen alleen aan dat vak mogen werken waarvoor ook een vakdocent aanwezig is. Maar meestal moet je als wiskundedocent leerlingen helpen die bijvoorbeeld met Engels of verzorging bezig zijn. Natuurlijk weet je wel genoeg om vragen te beantwoorden, maar op vakdidactisch gebied weet je te weinig van een vak dat niet het jouwe is. Uiteindelijk komt dit niet aan de leerling ten goede. Om de vorderingen van de leerlingen bij te houden wordt van de docent verwacht dat hij een groot deel van zijn tijd bezig is met administreren, en dat is zonde van die tijd. En aan de andere kant wordt op sommige scholen wiskunde gegeven door docenten die niets met wiskunde hebben, maar, door urenteruggang, restuurtjes geven. Dit baart mij wel zorgen omdat wiskunde daarmee een sluitpost wordt. Door dit nieuwe onderwijssysteem zijn er minder of geen lesuren speciaal voor wiskunde, waardoor er nauwelijks tijd en aandacht is voor de spannende en uitdagende aspecten van het vak. De leerlingen zien een boek en minder vaak een inspirerende docent. Dat is jammer, want naast het boek kun je nog zoveel leuke wiskunde geven. Hoewel wiskunde het imago heeft van ‘moeilijk en saai’, kun je in je lessen laten zien en merken aan de leerlingen dat wiskunde niet stoffig en saai is, maar vooral leuk, ook al is het soms moeilijk.

Zijn alle veranderingen ook verbeteringen?

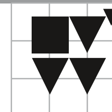
Er wordt veel van de leerling verwacht. Bedenk wel dat leerlingen, als ze bij ons binnenkomen, hooguit 12 jaar zijn. Kunnen we van vmbo-leerlingen verwachten dat ze zelfstandig een week vullen en plannen? Kunnen we verwachten dat ze bedenken wat ze wanneer in de week doen en dat ze de discipline hebben om wat langer met een vak dat ze moeilijk vinden, bezig te zijn? Het is immers veel leuker om aan een vak te werken dat je goed kunt… Hebben onze leerlingen genoeg zelfreflectie om te zien wat ze beheersen en waaraan ze nog wat aandacht moeten besteden? Als er op de basisschool in groepjes werd gewerkt, dan waren de vmbo-leerlingen sneller geneigd om mee te liften in

de groep omdat de vwo-leerlingen sneller het voortouw namen.
Wat de organisatie betreft moet aan een aantal voorwaarden voldaan worden: om het nieuwe onderwijssysteem in goede banen te leiden is er veel begeleiding nodig. Het is mijns inziens nodig om een onderwijsassistent in te zetten. Deze assistent kan veel administratieve taken doen. Er is daarnaast bijscholing voor docenten nodig omdat de taak van de wiskundedocent anders is dan bij het traditionele onderwijs: de docent wordt meer coach dan didacticus. Zeker de wat oudere docenten hebben dat niet in hun opleiding meegekregen en zullen moeten bijscholen opdat ze ook weer met kundigheid en plezier hun nieuwe taak kunnen vervullen.

Tot slot

Waarschijnlijk vinden leerlingen het leuker om in groepjes te zitten dan in de busopstelling, maar is het daardoor ook moeilijker voor ze om de discipline op te brengen om de gestelde taak en op tijd af te krijgen. Wat de docenten betreft is het de vraag of elke docent zit te wachten op een omschakeling naar een ander onderwijsconcept en een bijbehorende andere invulling van zijn of haar taak.
Ik denk niet dat we de optimale didactiek van de wiskunde al gevonden hebben; we zullen met z'n allen nog flink aan de slag moeten om voor iedere school een passende onderwijsvorm te vinden. Het is niet de vraag óf we aan de slag gaan; het is wel een uitdaging om aan de slag te gaan. Vanuit het bestuur gaan we scholen bezoeken om te kijken wat we kunnen doen voor docenten in het vmbo. We hopen dat u ons kunt helpen om als bestuur van de NVvW nog meer te doen voor het vmbo. Daarom wil ik graag in contact komen met mensen die een duidelijke visie hebben en die willen nadenken over het moderne wiskundeonderwijs.
De vereniging biedt nascholing, mogelijkheid tot informatie uitwisseling en contacten met andere docenten. Deze elementen zijn nodig voor een betrokken, vitale en inspirerende docent. Ook voor vmbo-docenten kan de vereniging veel betekenen.

Over de auteur
Henk Bijleveld is bestuurslid van de NVvW voor het vmbo en wiskundedocent op de Meerwaarde in Barneveld, een school voor vmbo-onderwijs.
E-mailadres is: *h.bijleveld@nvvw.nl*



OPROEP / AAN DOCENTEN OM ACTIEF DEEL TE NEMEN AAN DE STUDIEDAG

Het thema van de NVvW studiedag:
Wiskunde, daar kun je op rekenen!
Datum: **zaterdag 7 november 2009**

Doorlopende leerlijnen en aansluitingsproblematiek zijn meer dan ooit, mede door de aanhoudende politieke aandacht voor met name wiskundeonderwijsland, een hot item. Dat een en ander niet echt goed gaat wisten we al, maar hoe goed weten we wat er aan beide zijden van de scheidslijnen aan onderwijs wordt gegeven en genoten? En wat weten we van de keuzes die zijn gemaakt, onder andere door een beperkte hoeveelheid onderwijstijd? Volgens ons levert dit genoeg stof op voor discussie en informatie-uitwisseling op de studiedag.
Een paar voorbeelden:

- Weten we in het vo wel goed hoe er in het po wordt gerekend? Denk bijvoorbeeld aan alle krantenkoppen waarin de staartdeling wordt genoemd als verloren goed uit een rijk verleden. Is dat echt zo? En wat wordt er dan nog wel aan delen gedaan in het po?
- De commissie Meijerink met zijn referentieniveau's; er wordt veel geld uitgetrokken om het rekenen weer op peil te krijgen. Op individuele scholen wordt er aan gewerkt, Cito maakt toetsen, het APS en het FI verzorgen cursussen, de vereniging heeft twee rekenprojecten (voor vmbo en havo-C&M) en ook cTWO spreekt een woordje mee. Maar wat is eigenlijk functioneel rekenen en op welke manier besteed je daar aandacht aan; in de wiskundeles of daarnaast? En moet het ook functioneel zijn bij andere vakken? Hoe toets je het?
- Wat weet een bovenbouwdocent nog over wat wel en wat niet wordt behandeld in de onderbouw? Parallel daarmee: wat weten vmbo- en mbo-docenten van elkaars manier van wiskunde onderwijzen?
- En natuurlijk: hoe zit het met de algebraïsche vaardigheden in de overgang vo/ho. Hoe zijn de eerste examens van de 2007-programma's gevallen (of voelde het veld zich overvallen?) en wat mag er worden verwacht van de 2010-examens vwo? Hoe staat het met de vo/ho-dialoog over de aansluitingsproblematiek?

Allerlei (vervolg)opleidingen vinden dat je op wiskunde moet kunnen rekenen. En ook het rekenen moet op orde zijn. Kunnen wij dat blind garanderen of is het goed om daar wat genuanceerder over te praten?
Wij zullen een aantal personen en instellingen vragen een bijdrage te leveren aan de studiedag.
We willen ook graag informatie en discussie, direct vanuit het veld, een plaats geven.
Daarom roepen we hierbij u als docent op aan ons door te geven wat u zou kunnen en willen bijdragen aan het welslagen van de studiedag.
U kunt uw idee voorleggen aan één van de onderstaande personen. Als uiterste datum daarvoor hanteren we 15 juni 2009. De gehele studiedag moet namelijk voor de zomervakantie zijn ingevuld.
Wij hopen op veel goede, constructieve reacties.

De organisatoren van de studiedag zijn:

- Lidy Wesker, lerarenopleiding ILO van de UvA (*th.wesker@quicknet.nl*)
- Kenneth Tjon Soei Sjoe, lerarenopleiding wiskunde HvA-OO (*k.j.tjon.soei.sjoe@hva.nl*)
- Henk van der Kooij, bestuur NVvW (*h.v.d.kooi@nvvw.nl*)

Puzzel 84-7

Faculteiten!

[Frits Göbel]

$$C(n) = \frac{(2n)!}{(n+1)! \cdot n!}$$

Een eenvoudig gevolg van het feit dat alle binomiaalcoëfficiënten geheel zijn, is:
$a!b! \mid c!$
voor alle positieve a, b, c met $a + b \leq c$.
(Voor alle zekerheid: $d \mid n$ betekent: d is een deler van n.)

We willen nu eens onderzoeken wanneer $a!b! \mid c!$ geldt met $a + b > c$.
Een eerste voorbeeld is $a = n$, $b = 1$, $c = n$.
Om van dit flauwe geval af te zijn, nemen we van nu af $a > 1$ en $b > 1$.
Een beter voorbeeld wordt gevormd door de Catalan-getallen. Deze zijn geheel, dus $a!b! \mid c!$ geldt ook als $a = n + 1$, $b = n$, $c = 2n$.
Als c zelf een getal van de vorm $n!$ is, hebben we de oplossing $a = n! - 1$, $b = n$, $c = n!$, bijvoorbeeld $a = 23$, $b = 4$, $c = 24$. Hier geldt zelfs $a!b! = c!$.

Een tripel (a, b, c) dat voldoet aan $a!b! \mid c!$, noemen we *maximaal* als noch $(a + 1)!b!$ noch $a!(b + 1)!$ een deler is van $c!$.
Bijvoorbeeld, de maximale tripels met $c = 12$ zijn: (11, 3, 12), (9, 5, 12) en (7, 6, 12).
Het zal duidelijk zijn dat deze maximale tripels voldoende informatie geven over de verzameling tripels die voldoen aan $a!b! \mid c!$.

Opgave 1
Bepaal alle maximale tripels $(a, b, 18)$ met $a \geq b$.

Opgave 2
Bepaal de maximale tripels $(a, b, 2n)$ met $a \geq b > n$ en $2n < 200$.

Het is voor deze opgaven niet nodig om $n!$ te bepalen voor 'grote' waarden van n. Het is voldoende om voor bepaalde priemgetallen p de exponent van p in $n!$ te bepalen, en dat is niet moeilijk. Deze exponent wordt namelijk gegeven door:

(Met $\lfloor a \rfloor$ bedoelen we het grootste gehele getal kleiner dan of gelijk aan a; de *entier*-functie of *int*-functie.)

Het kan zelfs nog eenvoudiger, zonder machten van p uit te rekenen, met de volgende algoritme:

```
read n; read p;
t := 0;  q := int(n/p);
while q > 0 do begin
   t := t + q;  q := int(q/p)
end;
print t.
```

Oplossingen kunt u mailen naar *a.gobel@wxs.nl* of per gewone post sturen naar F. Göbel, Schubertlaan 28, 7522 JS Enschede.
Er zijn weer maximaal 20 punten te verdienen met uw oplossing.
De deadline is 30 juni 2009.
Veel plezier!

Oplossing 84-5

Bissectrices

Ondanks de verkeerde deadline waren er 22 inzenders, onder wie 3 nieuwe: Klaas Wijnia, Kees Jonkers en Hessel Pot. Hartelijk welkom!
De deadline is later op de website van *Euclides* verzet naar 7 april; misschien hebben sommigen dat gezien.

Het antwoord op *opgave 1* is:

$$\sqrt{\frac{ab(a+b-c)}{a+b+c}}$$

Ik gebruikte hierbij $AF/BF = a/b$ en een formule voor de lengte van een bissectrice:
$CF^2 = ab - AF \times BF$
En natuurlijk is AH een bissectrice in driehoek AFC. Vele anderen gebruikten de cosinusregel.

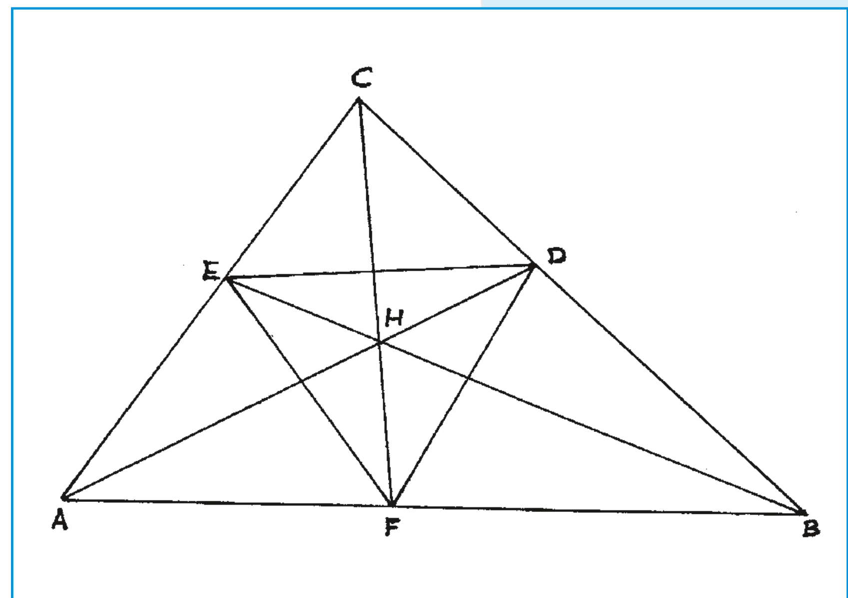
Niels de Bruin vroeg in hoeverre het nodig is om uitwerkingen in te sturen. Antwoord: dat is niet nodig, maar ik vind het wel prettig om een korte beschrijving van de gevolgde methode te zien. Verder geldt: een fout antwoord zonder enige toelichting is 0 punten, terwijl een fout antwoord met toelichting maximaal 20 punten oplevert.

Bij *opgave 2* hebben veel inzenders de zijden a en b geschreven als kp en kq, en vervolgens de hoogte van de driehoek met behulp van de formule van Heron uitgedrukt in k, p, q en c. Eén van de inzenders spreekt hier van een afschrikwekkende formule, die dan ook nog gedifferentieerd moet worden. Een wat elegantere afleiding loopt als volgt. Dankzij de gegeven verhouding kun je op AB de snijpunten F en G bepalen met de bissectrice en de buitenbissectrice. Deze twee deellijnen zijn onderling loodrecht, dus alle mogelijke plaatsen voor punt C liggen op de cirkel met middellijn FG. De maximale hoogte is dan de straal van die cirkel. Het antwoord is:

$$\frac{cpq}{|p^2 - q^2|}$$

Ook het antwoord op *opgave 3* werd op diverse manieren gevonden. Een eenvoudige methode gaat als volgt.
De oppervlakte van driehoek CDE is $k \times CD \times CE$, waarin k een constante is die alleen van hoek C afhangt. (In feite is k gelijk aan de helft van sin C.) CD en CE zijn eenvoudig in a, b en c uit te drukken. Het is handig om dit alvast te delen door de oppervlakte van driehoek ABC en hiervoor de formule kab te gebruiken. Dit levert dan $ab/(a + c)$. Cyclische verwisseling levert de andere twee 'puntjes'. De som van deze drie trek je af van 1 en dan verschijnt het antwoord:

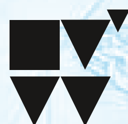
$$\frac{2abc}{(a+b)(a+c)(b+c)}$$



Ladderstand
De top van de ladder ziet er nu als volgt uit.
G. Riphagen 514
L. van den Raadt 415
H. Klein 412
W. Doyer 375
T. Kool 286
J. Hanenberg 277
N. Wensink 267
H. Linders 226
K. Verhoeven 217
M. Woldinga 214
W. van den Camp 200

SERVICEPAGINA

Publicaties van de Nederlande Vereniging van Wiskundeleraren



Zebraboekjes

1. Kattenaids en Statistiek
2. Perspectief, hoe moet je dat zien?
3. Schatten, hoe doe je dat?
4. De Gulden Snede
5. Poisson, de Pruisen en de Lotto
6. Pi
7. De laatste stelling van Fermat
8. Verkiezingen, een web van paradoxen
9. De Veelzijdigheid van Bollen
10. Fractals
11. Schuiven met auto's, munten en bollen
12. Spelen met gehelen
13. Wiskunde in de Islam
14. Grafen in de praktijk
15. De juiste toon
16. Chaos en orde
17. Christiaan Huygens
18. Zeepvliezen
19. Nullen en Enen
20. Babylonische Wiskunde
21. Geschiedenis van de niet-Euclidische meetkunde
22. Spelen en Delen
23. Experimenteren met kansen
24. Gravitatie
25. Blik op Oneindig
26. Een Koele Blik op Waarheid
27. Kunst en Wiskunde
28. Voorspellen met Modellen

Zie verder ook *www.nvvw.nl/zebrareeks.html* en/of *www.epsilon-uitgaven.nl*

Nomenclatuurrapport Tweede fase havo/vwo
Dit rapport en oude nummers van Euclides (voor zover voorradig) kunnen besteld worden bij de ledenadministratie (zie Colofon).

Wisforta – wiskunde, formules en tabellen
Formule- en tabellenboekje met formulekaarten havo en vwo, de tabellen van de binomiale en de normale verdeling, en toevalsgetallen.

Honderd jaar wiskundeonderwijs, lustrumboek van de NVvW
Het boek is met een bestelformulier te bestellen op de website van de NVvW: *www.nvvw.nl/lustrumboek2.html*
Voor overige NVvW-publicaties zie de website: *www.nvvw.nl/Publicaties2.html*

Voor overige internet-adressen zie ***www.wiskundepersdienst.nl/agenda.php***

Voor Wiskundeonderwijs Webwijzer zie ***www.wiskundeonderwijs.nl***

Kalender

In de kalender kunnen alle voor wiskundedocenten toegankelijke en interessante bijeenkomsten worden opgenomen. Relevante data graag zo vroeg mogelijk doorgeven aan de hoofdredacteur, het liefst via e-mail (*redactie-euclides@nvvw.nl*). Hieronder vindt u de verschijningsdata van Euclides in de lopende jaargang. Achter de verschijningsdatum is de deadline vermeld voor het inzenden van mededelingen en van de *eind*versies van geaccepteerde bijdragen; zie daarvoor echter ook *www.nvvw.nl/euclricht.html*.

nr.	verwachte verschijningsdatum	deadline
8	7 juli 2009	19 mei 2009

Voorlopige data 85e jaargang

1	22 september 2009	28 juli 2009
2	10 november 2009	15 sep 2009
3	22 december 2009	27 okt 2009
4	9 februari 2010	8 dec 2009

woensdag 3 juni, Utrecht
Centrale bespreking vwo B1/B12
Organisatie NVvW

woensdag 3 juni, Utrecht
Studiemiddag 'Rekenbeleid bij u op school'
Organisatie APS

donderdag 4 juni, op diverse plaatsen
Regionale bespreking vwo B1/B12
Organisatie NVvW

vrijdag 5 juni, Utrecht
Wiskunde D-dag
Organisatie cTWO

8, 15 en 22 juni (maandagen), Utrecht
Cursus Statistiek en Kansrekening voor Wiskunde D
Organisatie Fisme

vrijdag 12 juni, Utrecht
Studiedag TI-Nspire
Organisatie T3 Nederland en FIsme

vrijdag 19 juni, Utrecht
Workshops 'Bèta onder de Dom'
Organisatie Universiteit Utrecht i.s.m. BEST-Utrecht

ma. 17 t/m vr. 21 augustus, Utrecht
Utrecht Summer Schools in Science and Mathematics Education
Organisatie Universiteit Utrecht

vr. 21 en za. 22 augustus, CWI Amsterdam
vr. 28 en za. 29 augustus, TU/e Eindhoven
Vakantiecursus 2009 – Tel uit je winst
Organisatie CWI
Zie pag. 270 in dit nummer.

14 en 28 oktober, 11 november (woensdagen), Utrecht
Cursus Analytische Meetkunde voor Wiskunde D
Organisatie FIsme

zaterdag 7 november
Jaarvergadering/Studiedag: Op Wiskunde kun je Rekenen
Organisatie NVvW
Zie ook pag. 273 in dit nummer.